Affordable Cybersecurity for All
人人都能負擔得起的網絡安全

Interviewed by : Ms. Agnes Tan
採訪者：陳國萍小姐

Mr. Bernard Lee
Chief Executive Officer
BlueSky

李本立先生
行政總裁
藍天專業服務有限公司

Lee believes that everyone deserves security. It is the second layer of the Maslow's hierarchy of needs, right on top of food, air and water. Without safety and security, people degenerate to mere survival beings. Hong Kong is very lucky to be in a place recently named 9th safest city in the world (https://www.cw.com.hk/it-hk/hk-named-world-s-ninth-safest-city). However, the world is progressing in an alarming rate in terms of technology, communication and information availability; and while new doors are being open, along comes new channels for intrusion and deception. In the old days, property refers to our home, our cash, our jewelry, and protecting our loved ones and our property are mostly through traditional means. Today, property has taken the digital form more and more, and traditional means of protection is no longer enough. It is of paramount importance that those of us who are gifted with the knowledge and experience to contribute back to our society and make it a better place.

Lee believes that by far the biggest challenge is the commercial world's motivation to "productize" security. People don't stay safe riding a bike by just buying an expensive helmet. We stay safe through knowledge and behavior and experience. There is need for sustainable learning on how to stay safe in this digital era. Such CSR is costly and making such learning sustainable is a long-term investment. Figuratively, people should focus less on selling expensive helmets and more on sharing knowledge on how to ride a bike safely. Lee wishes to make a calling for more people who have the reach and resources to participate in this very important cause, so Hong Kong shall remain the one of the safest cities in the world through this digital era.

BlueSky's Contribution to Cybersecurity

BlueSky is currently developing a software platform for MSSP (Managed Security Service Provider). Similar to Uber or DiDi where customers can hire a ride without purchasing the car, clients can hire security service providers on-demand without

李先生認為每個人都應該得到安全保障。它是馬斯洛需求層次理論的第二層，在食物、空氣和水的基礎上。沒有安全和保障，人們就墮落至僅僅為生存了。香港很幸運最近被評為世界最安全城市的第九名（https://www.cw.com.hk/it-hk/hk-named-world-s-ninth-safest-city）。然而，在技術、通信和訊息可用性方面，世界正在以驚人的速度前進；當有新的科技誕生時，也會出現入侵和欺騙的新渠道。以往，財產泛指的是我們的房屋、現金、珠寶，要保護我們所愛的人和財產，主要是用一些傳統的方法。如今，財產已變得越來越數碼化，而傳統的保護方法已經不合時宜。最重要的是，我們擁有知識和經驗的人，應該回饋社會，使它成為一個更好的地方。

李先生認為，到目前為止，最大的挑戰是商業世界中「產品化」的安全動機。我們不會因為買了一個昂貴的頭盔便會安全地騎自行車。我們是靠知識、行為和經驗確保自身安全。在這個數碼時代，我們仍需要不斷學習如何保持安全。例如企業社會責任的成本很高昂，使這種可持續發展的學習成為一項長期投資。比喻，我們應該注重如何安全駕駛，而不是注重如何銷售昂貴頭盔。李先生希望呼籲更多有能力和資源的人參與，憑藉這個數碼時代使香港繼續成為世界上最安全的城市之一。

藍天專業服務有限公司對網絡安全的貢獻

BlueSky目前正為託管安全服務供應商（MSSP）開發一個軟件平台。與優步或滴滴類似，客戶無需購買汽車下租用車輛，客戶可以按需要而租用安全服務供應商，而無需購置整個服務。正因為如此，客戶處於共享經濟中，這個平台讓客戶，以及其他合資格、受過專業訓練的獨立網絡安全服務供應商，可以以高效率但較低的成本管理大量中小企業務。通過這一點，他們可以讓所有人使用負擔得起的網絡安全。為了讓網絡安全在共享經濟中可行，BlueSky的MSSP追踪系統可以知道誰幫

purchasing the whole security package. Because of this, they are in a sharing economy, and this platform shall let them, and other qualified and highly trained independent cyber security service providers manage lots of small to medium businesses at a lower cost because of efficiency. Through this, they can make cyber security available and affordable to everybody. To make cybersecurity feasible in a sharing economy, BlueSky's MSSP ticketing system intricately tracks who works for whom and what data different people can access. This tracking system serves as a bird's eye view of everyone's security (without assessing sensitive data) that details who can access private information. The system tracks unauthorized access and alerts BlueSky's staff when there are unexpected intrusions.

That being said, the model can be quite complex. For instance, customers can rent a server, but they also need to verify that the server is secure. Keeping a server secure is much more than buying firewalls. Some mandates (e.g. ISO 27001) state follow able guidelines such as separation of duties and facilities among development, testing and production. However, such guidelines, when combined with other security measures such as two-factor authentication, physical security and administrative procedures, can make proper implementation very intricate.

Fortunately, technology today is highly sophisticated such that the strongest computers cannot crack good encryption mathematically if they are done properly. Movies that feature hacking into advanced security systems within a short timespan are a myth. Hacking merely though a properly secured computer is impossible without the aid of social engineering (e.g. manipulating and deceiving people to obtain information). Hence, Lee advises enterprises to not only adopt cybersecurity services, but also defense against social engineering tactics. The biggest vulnerability is the human.

In addition to BlueSky, Lee is also Co-Chair of the Sustainable Business and Management Division, World Institute of Sustainable Development Planners (WISDP), which is part of UN and UNESECO. By taking the role at WISDP, he assumes the role of cyber security expert and influencer, bring what he knows and learned from his business, and collaborate with UNESCO and UN on leadership programs with universities, high schools, unprivileged communities and like-minded individuals by planting seeds on how they can contribute to UN Sustainable goals in their careers and daily lives. The goals Lee focus on are (9) Industry, Innovation and Infrastructure; (10) Reduced Inequalities; (16) Peace, Justice and Strong Institutions; and (17) Partnerships for the Goals. He collaborates with leaders within UNESCO and UN through his service, so they can in turn bring ideas to other leaders and future leaders to create a sustainable ecosystem for safety education in the information era.

Need for Cyber Education

Cyber education is crucial for public safety. Everyone has the social responsibility to tell others how to stay safe. The more we

誰辦事，什麼人可以讀取哪些數據進行複雜的追踪。這個追踪系統可以作為對每個人安全（沒有讀取敏感數據）的鳥瞰圖，了解誰可以讀取私人訊息。當出現突發入侵時，系統會跟踪未經授權的讀取，並向BlueSky的工作人員發出警報。

話雖如此，這個模型可能相當複雜。例如，客戶可以租用一台伺服器，但他們也需要驗證伺服器是否安全。保持伺服器的安全性遠比購買防火牆更為重要。一些授權（如 ISO 27001）規定了可遵循的指導方針，如在開發、測試和生產中分開職責和設備。然而，這些準則與其他安全措施，如雙重認證、實體安全和行政程序相結合，可以使正確的實施變得非常複雜。

幸運的是，今天的科技非常複雜，即使超級電腦都無法用數學方法破解良好的加密技術。電影中在短時間內入侵先進的安全系統絕對是一個神話。如果沒有社交工程的輔助（例如操縱和欺騙我們讀取訊息），僅僅通過一台安全的電腦來進行黑客攻擊是不可能的。因此，李先生建議企業不僅要採用網絡安全服務，還要防範社交工程手法。因為最大的漏洞就是人類。

除了BlueSky之外，李先生還是可持續發展商業和管理部門的聯合主席，世界可持續發展規劃師（WISDP），這是聯合國和聯合國教科文組織的一部分。通過在WISDP擔任職務，他充當著網絡安全專家和影響者，將他從商業中的所知所學，在聯合國教科文組織和聯合國合作的領導計劃中，為聯合國可持續發展的目標中指導各大學、高中、貧窮社區和志同道合人士，如何在職業生涯和日常生活中作出貢獻。李先生集中的目標是（9）產業、創新和基礎設施；(10) 減少不平等；（16）和平、正義和強大機構；（17）促進目標實現的伙伴關係。他通過自己職務與聯合國教科文組織和聯合國的領導人合作，如此他們就可以向其他領導人和未來的領導人提出想法，為訊息時代的安全教育創造一個可持續的生態系統。

網絡教育的需要

網絡教育對公共安全至關重要。每個人都有社會責任告訴別人如何保持安全。在數碼時代，我們做得越多，那些效仿的人也會和他們的朋友分享以及教育他們的孩子，很快整個生態系統便可持續了。儘管有很少公共垃圾桶的日本也若能成為世界上最乾淨的國家之一，那麼香港也可以不需要每個人都購買大量的產品，而成為世界上網絡安全的城市之一。這就是教育的作用。

最近，Frost和Sullivan為網絡安全和教育中心進行的一項研究顯示，在不久的將來，全球網絡安全人員將面臨66%的短缺。造成全球短缺的關鍵因素是（a）缺乏合資格人員；（b）領導人之間的理解不足；（c）缺乏商業預算；（d）難以挽留合資格人員；（e）缺乏職業發展前景。在2016年的Gartner報告中，排名前三的網絡安全諮詢公司分別是德勤、安永和普

do it, with the digital age, those who learn will also share with their friends and educate their young, and soon the whole ecosystem will be sustainable. If Japan can be one of the cleanest countries in the world despite very few public trash cans, Hong Kong can become one of the cyber-safe cities in the world without everyone buying lots of products. It is all in Education.

In a recent study by Frost & Sullivan for The Center for Cyber Safety and Education, there will be a 66% global shortage of cyber security personnel in the near future. The key factors contributing to the global shortage are (a) shortage of qualified personnel; (b) insufficient understanding among leaders; (c) lack of budget in business; (d) difficulty retaining qualified personnel; and (e) lack of career path in the industry. In the 2016 Gartner report, the top 3 cyber security consulting firms are Deloitte, EY and PwC, with 2.857 billion, 2.036 billion and 1.947 billion US dollars in cyber security revenues respectively. In Asia in particular, there are arguably no affordable quality services that can be compared against the big players. This is equivalent to saying that there is a huge market for cars, but 90% of the cars sold are luxury cars, and economy cars are not available because nobody makes them. People should learn about new technology in this digital age and prioritize security over the latest trends, such as cryptocurrency.

Cryptocurrency and Its Potential Threats

Cryptocurrency and Crypto investment scams have gotten vast public attention and may become a bigger threat in the coming years. Though Lee does not view cryptocurrencies and ICOs as scams by themselves, they are not maturely regulated and can become opportunities for fraud and scamming when put in the wrong hands. Here is Lee's humble opinion for the general public:

(a) When strangers or friends call or message you and say "hey, buy this crypto, it will go up", it is equivalent to saying to you "give me X dollars and you will own Y shares in this company". If you were asked the later question the first questions people may ask: What does the company do? How will it make money? Who is running it? What are the risks? Unfortunately, many people, when asked the first question, may instead ask: Really? Are you sure? How do I buy? When someone, even a friend, ask you to buy a coin, inquire as if they are asking you to invest money in a company.

(b) There are Pre-ICO coins and Post-ICO coins. They are equivalent to buying shares in a private company vs. a listed company, except for the fact that neither are currently maturely regulated by governments. Remember you will not likely be able to sell your Pre-ICO crypto easily once you buy it. Again, treat buying crypto as if you are investing in a company. Ask the right questions, and if you don't know the right questions to ask, but still want to invest in crypto, start with the most well-known cryptos.

(c) When you buy a crypto even on a reputable platform, remember that in many of these platforms, you do not actually own the crypto. If you buy cryptos from them, you buy a "position".

華永道，網絡安全收入分別為2.857億、2.036億和1.947億美元。特別是在亞洲，可以說沒有負擔得起的優質服務可以與大公司相比。這就相當於說，有巨大的汽車市場，但90%的汽車都是豪華轎車，而市場上則無人生產經濟型轎車。我們應該在這個數碼時代學習新技術，並優先考慮安全問題，而不是關注最新潮趨勢，比如加密貨幣。

加密貨幣及其潛在威脅

加密貨幣和虛擬貨幣投資騙局已經引起了公眾的廣泛關注，並可能在未來幾年成為更大的威脅。儘管李先生並不認為加密貨幣和ICOs是一種騙局，只是它們並未有成熟的監管，所以當處理不當時，便可能成為欺騙和欺詐的機會。以下是李先生給公眾的一些淺見：

（a）當陌生人或朋友打電話或發訊息給你，說「嘿，買這個虛擬貨幣，一定升」，這相當於對你說「給我X元，你就會擁有這家公司Y數量的股份」。如果你被先問後者的問題，我們可能會第一時間問：這間公司是做什麼的？他們如何賺錢？誰營運此公司？ 有什麼風險？不幸的是，當我們被問到前者問題時，許多人可能會問：真的嗎？你確定嗎？ 我怎麼買？當某人，甚至是朋友，要求你買一枚硬幣，他們是否要求你對一家公司作投資。

（b）市場上分別有上市前首次代幣發行（Pre-ICO）硬幣和上市後首次代幣發行 (Post-ICO) 硬幣。它這相當於購買一家私人公司的股票，而不是一家上市公司的股票，除非這硬幣已經受到政府的嚴格監管。記住，一旦你買了它，你就不可能輕易地賣掉你的Pre-ICO虛擬貨幣。再者，購買虛擬貨幣就像你在投資一家公司一樣。問正確的問題，如果你不知道正確的問題，但仍然想要投資虛擬貨幣，請從最著名的虛擬貨幣開始。

（c）當你在一個聲譽良好的平台上購買虛擬貨幣時，請記住大多數這些平台，你實際上並沒有擁有虛擬貨幣。如果你從這些平台購買虛擬貨幣，你只買了一個「狀態」。你不能自己出售虛擬貨幣的「狀態」。如想取回你的錢，你必須「關閉購買的狀態」，這意味著你必須遵守它們所有的規則和政策，然後才能把錢拿回來。規則和政策包括處理費，最小交易數量，等候時間，並且他們只會把錢經特別渠道退回。當你想購買一個“虛擬貨幣狀態”之前，確保已仔細閱所有難明的條款。

（d）當你真的買了一枚硬幣（而不是一個「狀態」）時，它必須存儲在一個虛擬貨幣錢包裡。虛擬貨幣錢包可以是流動應用程式、網絡應用程式、電腦應用程式、虛擬貨幣硬件錢包，或者甚至可以是一張像錢一樣的紙，上面有兩個二維碼（一個「虛擬貨幣錢包」）。由於所有虛

You cannot sell the crypto "position" on your own. To get your money back, you must "close the purchased position", meaning that you must follow all their rules and policies before you can get your money back. The rules and policies include handling charges, minimal transaction size, wait time, and that they will only deposit money back in certain channels. Make sure you read all the fine prints before you buy a "crypto position"

(d) When you actually buy a coin (as opposed to a "position"), it must be stored in a crypto wallet. The crypto wallet can be a mobile app, a web app, a PC app, a hardware wallet, or can even be just a piece of paper like money with two QR codes on it (a "Paper Wallet"). Since all crypto wallets deal with encryption, and most of them are not yet government regulated, the list of safe, reputable crypto wallets is only spread through word of mouth and trust. So, if you don't understand how a crypto wallet works, be careful on whom you trust.

(e) All crypto wallets use a Private Key. For paper crypto wallets, never ever let people take a picture of your QR codes, or your money is good as gone. Otherwise, a paper crypto wallet is probably the safest way for you to store crypto. For crypto wallet apps, make sure you don't jailbreak or root your phone, and keep your firmware version updated so the latest security holes will be patched in time. For web or PC based crypto wallets, never let a people you don't trust use your computer. Take out/destroy your hard drive before you sell or discard your old computer. For hardware wallet, it is your money, and if you lost or damaged your hardware wallet, your money is gone either, so keep your hardware wallet as if you keep your diamonds and jewelry.

All in all, one must understand crypto at a conceptual level before spending money on it, and if you have difficulty understanding it, find someone you trust in real life who really understands it, and act as if you give them cash to invest in someone's company.

Telephone Deception

While telephone scams still come from cold calls from strangers, scams have evolved to take on messages (e.g. Whatsapp, WeChat, Skype, Facebook) and 'weak/temporary contacts' via social networking. According to Lee, all of the recent breaches happen for a reason. Hackers and identity thieves are way ahead of us. The more they know about us, the easier they can manipulate us by tricking us into believing us that they are real, when in fact they are not. Imagine the scenarios:

(a) We are XXX travel agency. Your flight next week to YYY is oversold. We apologize for the inconvenience. As a loyal customer for Z years, we are pleased to offer you a free upgrade to business class. We need to authorize your credit card for the small handling fee.

(b) We are AAA bank. We have reason to believe that your online banking account is compromised. We shall send you an SMS to your registered phone. When received, do not tell us the

擬貨幣錢包都有加密處理，而且其中大多數還未受到政府的監管，因此，安全、有信譽的虛擬貨幣錢包名單只會靠口碑和信譽傳播。所以，如果你不明白虛擬貨幣錢包是如何使用，那就小心你信任的人。

（e）所有虛擬貨幣錢包都使用私鑰。對於虛擬貨幣錢包，絕對不要讓別人拍下你的二維碼，不然你的錢就被轉走了。否則，虛擬貨幣錢包是存儲虛擬貨幣的最安全的方法。對於使用虛擬貨幣錢包應用程式，你必須確保手機不會越獄或解鎖，並保持更新固件從而取得及時修補的最新的安全漏洞。對於網頁版或電腦版的虛擬貨幣錢包，永遠不要讓你不信任的人使用你的電腦。在你賣掉或丟棄你的舊電腦之前，先把你的硬盤拿出來或銷毀。對於虛擬貨幣硬件錢包來說，如果你丟失或損壞了你的虛擬貨幣硬件錢包，你的錢也會消息，所以保護你的虛擬貨幣硬件錢包就像你保護你的鑽石和珠寶一樣。

總而言之，你必須在概念層面上理解虛擬貨幣才好花錢去買它。如理解它感困難，那就請教一個你信任並且真正了解虛擬貨幣的人，並當作你把錢給他們去投資某人的公司一樣的查問。

電話騙案

雖然電話騙案都是來自陌生人來電，但詐騙已經演變為通過社交網絡獲取訊息（如Whatsapp、微信、Skype、Facebook）和「弱/ 臨時聯繫」。根據李先生的說法，最近所有的騙案事件發生都是一個原因。就是黑客和身份竊賊遠遠領先於我們。他們對我們了解得越多，他們就越容易操縱我們，欺騙我們，讓我們相信他們是真實的，而事實則相反。想像一下以下的情景:

（a）我們是XXX旅行社。你下星期飛往YYY的航班被超賣了。我們很抱歉給你帶來不便。閣下已是我們Z年的長期客戶，我們很高興為您提供免費升級到商務艙。我們需要你授權你的信用卡支付小額的手續費 。

（b）我們是AAA銀行。我們有理由相信你的網上銀行賬戶已被盜用。我們將向你登記之電話發送短訊。當收到時，不要告訴我們你的密碼。我們同時也會通過你的登記電郵地址發送「密碼重置」鏈接給你，請點擊，並輸入你的6位授權碼來重置你的在網上銀行密碼。

這些只是部份可能發生的例子，它們利用「弱聯繫」來利用受害者的絕對信任，也就是那些你不認識的人，他們代表的是你所知道的公司或服務。這類型的騙局使用的技巧叫做「魚叉式網絡釣魚」和「社交工程」，可以來自電子郵件、社交媒體、即時通訊、短訊、電話或任何其他類型的數碼通訊。

password. Click on the password reset link, which we will also send you via your registered email and enter your 6-digit authorization code to reset your online banking password.

These are just some of the many possible examples that exploit the implicit trust of victims via "weak contacts" i.e. people whom you don't know whom represent a company or service that you know. These types of scams use techniques called "Spear Phishing" and "Social Engineering", and can come from email, social media, instant messaging, SMS, phone calls, or any other kind of digital communication.

Lee provides one simple for the general public: if anyone ask for your private information, such as passwords, authorization code, phone number, credit card number, or send you any link to reset or enter such private information, refrain from reacting directly. Courteously say you are currently busy and will call them back. Instead of calling them back, take the trouble, go to your bank branch, telecommunication provider branch, or service provider office, and ask to speak to their staff or manager on duty, and ask them if they initiated the communication. Most often than not, you would have avoided being victim of Cybercrime and Telephone Deception.

Most importantly, when one's teenage children start to fall in love with social networks and messaging, find ways and means to credible information on how to keep them safe from cyber malice. It is very difficult with the modern generation gap where teenagers realize that they are a lot more tech savvy then their parents and often mistakenly conclude that they know better than to listen to their parents on these topics as well.

What Service Providers Can Do to Prevent Cybercrime

Security and privacy can be a double-edged sword. When we are out on the streets and if the police force sees us, we feel safe. What about in the telephone or cyber world? How do we feel if what we do and what we say are being "heard" or "seen"? Without taking sides, Lee shares humble opinion on how an industry leader can step up.

(a) Start with transparent end-user license agreement and privacy promises and promote those actively. Take a side, have a soul and a personality. We may lose some customers, but those who remain will be extremely loyal advocates.

(b) Provide options. Those who engage in motorsports or climb the Everest exercise their right and freedom to take a risk. Those who bring bodyguards to their private meetings trade privacy for safety. We are lucky enough to be in a place with freedom of speech and choice. Provide it.

(c) Consider being an innovator and hence the leader. We are in the age of Artificial Intelligence. Emotional analysis through image recognition, behavioral analysis through screen swipes

李先生為大眾提供了一個簡單的方法：如果有人要求要你提供私人資料，比如密碼、授權碼、電話號碼、信用卡號碼，或者發送任何鏈接來重置或輸入你的私人資料，請不要直接作出回應。只需要禮貌地說你現在很忙，會給他們回電話。但不要再打電話給他們，直接到你的銀行分行，電訊供應商分店，或者服務提供商的辦公室，要求和他們的員工或經理查詢，問問他們是否曾致電給你。往往在這情況下，你便會避免成為網絡犯罪和電話騙案的受害者。

最重要的是，當一個青少年開始愛上社交網絡和訊息傳遞時，從可靠的資訊中尋找方式和方法，來告訴他們如何免受網絡惡意攻擊，但因代溝問題使難以進行，因青少年認為他們自己比父母更精通技術，並且經常錯誤地認為，比起聽取父母的建議，他們自己了解的更多。

服務提供商可以做些什麼來防止網絡犯罪

安全和隱私可能是一把雙刃劍。在街上，看到警察會感到安全。在電話或網絡世界裡呢？如果我們所做的和所說的被「聽到」或「看見」，我們會有什麼感受呢？李先生分享一些拙見作為一個行業領袖如何能加強防止網絡犯罪。

（a）從一目了然的用戶服務合約和私隱承諾開始，並積極推廣。堅守信念和個性，我們可能會失去一些客戶，但那些留下來的人將是非常忠誠的支持者。

（b）提供選擇。那些從事賽車運動或攀登珠穆朗瑪峰的人都有權利和自由去冒險。那些以私隱換取安全的人，把保鏢都帶到私人會議上。我們很幸運，能在一個言論和選擇自由的地方。提供我們選擇的權利。

（c）考慮成為一名創新者，從而成為領導者。我們正處於人工智能時代。通過圖像識別、屏幕滑動、點擊和按鍵來作行為分析、通過區塊鏈的信譽權威、通過自然語言處理的意圖和惡意意圖等來進行情感分析，這些都相當於現代通訊的「防毒軟件」。當變得更實惠和主導行業時，使用它。

（d）教育。服務提供商不會監視他們的客戶。他們為我們的客戶提供了安全和私隱的選擇自由。為可持續安全教育提供訊息和資料，並提供產品以協助執行網絡安全的最佳典範。

綜上所述，大膽的行業領袖可以令公眾受益，並使香港繼續在資訊時代成為世界上最安全的城市之一。那些在非政府組織或服務機構中的領袖，應該大膽地向政府和媒體發聲，並同時考慮促進企業社會責任的教育項目的積極認可和推廣。

and clicks and keystrokes, credibility authority through blockchain, intent and malicious intent through natural language processing, are all the equivalent of "antivirus" for modern communications. Apply as they become affordable and lead our industry.

(d) Educate. Service providers are not spying on their customers. They provide the freedom of choice to our customers – safety and privacy. Provide information and material for sustainable safety education and offer products to assist in enforcing the best practice for cyber safety.

In sum, daring industry leaders can benefit the general public and continue to make Hong Kong one of the safest cities in the world in the information age. Those who have roles in an NGO or service organization should speak up to our Government and Media and also consider contributing to the positive endorsement and promotion of the CSR education programs.