Professional Cybersecurity Expert to Combat Professional Hackers

專業網絡安全專家對付專業黑客

Interviewed by : Mr. Vincent Kwok

採訪者：郭榮忠先生

Mr. Vincent Ma
Chief Executive Officer
WTT HK Limited

馬惟善先生
行政總裁
滙港電訊

Established in 1995, WTT HK Limited (WTT), possessing significant fixed-line infrastructure in Hong Kong, is the only enterprise-focused fixed telecommunication and ICT services operator. WTT has already invested over HKD7 billion in its network to create a leading fiber-optic end-to-end network serving 90% business customers in Hong Kong. Together with a robust in-house service engine offering a comprehensive range of ICT products and bespoke solutions, WTT is an entrusted business partner across industries. In a dynamic and competitive business environment, enterprises are under more pressure than ever to adapt to new technology. Embracing cloud is the trend and cybersecurity naturally becomes the key concern for all businesses in this cloud connected era.

Cybersecurity is important to all businesses. As the leading ICT service provider in the region, WTT is dedicated to creating a secured and trusted cyber environment to enable enterprise development and to build successful business. WTT believes that the only way to win and grow is to help customers win.

Changing of Cyber Threat Landscape Impels Cybersecurity Evolution

According to Ma, cybersecurity was not a top agenda 20 years ago for most businesses, especially SMEs. Today, however, the changing threat of cyber environment impacts all industries, including some that may have never considered themselves as targets. The shock of cyber-attack becomes intensive and disruptive, extending well beyond financial implications. Increasingly, cybersecurity needs to be acknowledged as the top and key concern for all businesses.

One of the major challenges of cybersecurity for business today is that rapid development of mobility technology melting down the existing security measures. Most corporations nowadays allow executives to access critical company data via their smart devices which are not sufficiently protected by the company's firewall, for convenience and efficiency but compromising data security.

滙港電訊有限公司（WTT）成立於1995年，是本港唯一專注服務商業客戶的固網及資訊及通訊科技（ICT）服務營辦商。WTT投資超過70億港元自建具規模的固網基礎設施，擁有覆蓋全港90%商業客戶的「直達桌面」光纖寬頻網絡基建；再配合強大的專業服務團隊及一系列的ICT產品及解決方案，是各行各業值得信賴的合作夥伴。於這個競爭激烈及瞬息萬變的營商環境中，企業於接受及採用新技術的壓力確實比以往大；隨雲端之普及，網絡安全也成為企業非常重視的議題。

網絡安全對各行各業至關重要。WTT為香港具領導地位的ICT服務供應商，力臻締造安全可靠的網絡環境，讓企業發展業務。WTT深信致力協助客戶在其業務取得成功，脫穎而出，並與客戶一起成長，就是公司取得成功的不二之道。

WTT provides Multi-Cloud Solutions & Unified Communications services to Hong Kong business customers.

Mobility puts pressure on IT department as it creates complexity of network environment which requires more resources and knowledge to ensure the safety of business data which can be assessed anywhere anytime in this cloud era.

Moreover, cyber-attacks become more sophisticated. Attackers tend to take multi-step or multi-stage attack to achieve their criminal objectives. The nature of intrusion creates difficulty for detection. Phishing scam is a common multi-step attacking tactic that constitutes a major type of cyber-threat.

Another key attack target unique to business is supply chain network. Electronic data processing facilitates information exchange between organisations, which constitutes a supply chain of network with a higher level of interdependence and connectivity where a large amount of sensitive business data exchanges every minute. Any weaker link in the supply chain can grant the attacker access to the organization in custody of the data. The impact of supply chain network attack can extend to a large number of companies which is devastating.

The situation is getting worse because enterprises are not facing amateur attackers but criminal organizations from the dark side of Internet. The proliferation of cybercrime has reached the point where cybercrime-as-a-service is now a business; people hire organized and well-equipped hackers with a whole array of cyber-attack "service" to hack a given target. These cyber-attacks mainly consist of ransomware, distributed denial-of-service, phishing, and malware. Today, cybercrime is becoming increasingly commercialized; sophisticated cyber-attacks tend to target enterprises (such as financial institutions) for monetary benefits.

Despite the fact that most businesses now begin to recognize the importance of cybersecurity, only 8% of Hong Kong companies employ information security staff, and less than 3% of information security management systems have proper incident response mechanisms. Logically, enterprises with less cybersecurity resource input are bearing the brunt of cyber threats. Enterprises are in need of professional security personnel to deal with proficient

威脅日新月異　網絡安全需與時並進

馬先生指，二十年前，對大部分公司尤其中小企而言，網絡安全不是首要考慮的事項。可是，時至今日，網絡環境下的威脅不斷演變，對各行各界均造成影響，一些從未視自己為受攻擊目標的企業亦不能倖免。網絡攻擊所帶來的衝擊強烈，破壞力強，所造成的影響不啻於財政事務。網絡安全已逐漸被所有企業視為首要關注的議題。

流動技術蓬勃發展，令現有的資訊保安措施大受考驗甚至悉數瓦解，隨之成為當今企業面臨的一大網絡安全挑戰。現時，大多數企業為了換取方便和快捷，允許員工以智能設備存取公司關鍵數據，但這些設備卻未受公司的防火牆充分保護。流動技術使網絡環境複雜化，令IT部門備受壓力。企業需要運用更多資源及具備專業知識，才可確保隨時隨地從雲端安全地存取商業數據。

此外，網絡攻擊日趨精密。黑客傾向採取多重步驟或多重階段攻擊來達成犯罪目的，要偵測入侵行為絕非易事。網絡釣魚詐騙就是常見的多重步驟攻擊手段，亦構成網絡安全的一大憂患。

另一個只瞄準企業的主要攻擊目標就是供應鏈網絡。電子數據處理（EDP）有利機構之間的資訊相互交流，構成相互倚賴及連接的供應鏈網絡，每分鐘交換大量敏感的商業資料。只要供應鏈中出現任何較弱的連結，都可讓黑客藉機侵入，並存取機構所保管的數據。入侵供應鏈網絡造成的影響更可牽連至多家企業，後果不堪設想。

由於企業並非面對業餘的攻擊者，而是來自網絡世界陰暗一面的犯罪組織，情況因而變得愈來愈嚴峻。網絡罪案已醞釀成一種商業服務；不法分子聘請有組織、技術設備精良的黑客，並以一系列網絡攻擊「服務方案」來入侵既定目標。這些網絡攻

WTT is a trusted partner to businesses in strengthening cybersecurity management.

organized hackers skilled in hacking enterprises' valuable data. Alternatively, enterprises may rely on professional managed services and advanced technology to overcome the cybercrime challenges. By bringing together a diverse set of technologies and domain know-how across different sectors, professional security services providers can tackle the situation by creating an intelligent and highly secure environment for enterprises.

WTT's Approach to Combat Cybercrime

WTT anticipated a surge in information security service demand and launched Asure Security managed security services to keep businesses safe from cyber-attacks. As an all-round Managed Security Services Provider (MSSP), WTT not only offers a series of managed cybersecurity services with their Security Operations Centre (SOC), but also provides compliance consultancy for businesses to strengthen information security management for clients in long-term. WTT has now assisted companies from various industries, including financial services, healthcare, logistics, retail and travel, etc., to strengthen cybersecurity management and comply with the latest regulatory of authorities.

According to Ma, the provision of cybersecurity services is an on-going and dynamic business, with changing concerns according to client's company scale, level of digitalization, network complexity, cloud adoption and many other factors. That is why WTT had designed a highly customizable, easy-to-start and all-inclusive Asure Security packaged service to meet their IT security policies and stringent authority regulations across business fields. Asure Security offers round-the-clock monitoring plus top-of-class UTM firewall and advanced threat prevention (ATP) technology to build up solid and proactive front-line defense. Well-defined Security Information and Event Management (SIEM) performs quick capture, high-powered analysis, integrated threat correlation and wide-range malware identification which have made Asure Security surpassing traditional SIEM-based security solution.

WTT has cybersecurity teams that master a broad spectrum of technologies available for cybersecurity and possess in-depth understanding of mission-critical needs of different businesses, having established a proven track record of addressing the cybersecurity needs of financial institutions operating in stringent regulatory environment. WTT is more than ready to be a trusted partner and a digital security expert that can master technology trend with proven credentials to help companies combat any potential cyber-attacks.

Cybercrime and CSR

The future of business lies within a wholly digital and connected world. Without sufficient cybersecurity measures in place to manage and protect enterprises' data, businesses run the risk of overexposure and vulnerability for exploitation.

WTT believes that Corporate Social Responsibility (CSR) and business objectives can co-exist; their mission is to deliver business value by thinking innovatively and embracing long-term sustainable effort to economic, social and environmental impacts

擊主要包括勒索軟件、阻斷服務攻擊（DDoS）、網絡釣魚詐騙和惡意軟件。時至今日，網絡犯罪逐漸變得商業化，而精密嚴謹的網絡攻擊亦傾向以企業為目標，譬如財務機構，以獲取金錢上的利益。

儘管大多數企業開始意識到網絡安全的重要性，卻只有8%的香港公司有聘用資訊保安人員，少於3%的資訊安全管理系統設有完善的事故應變機制。由此可推斷，於網絡安全方面不甚投放資源的企業將會首當其衝，遭受網絡威脅。企業需要信賴專業的資訊安全管理人員，以應對擅於竊取公司寶貴資料的有組織專業黑客。企業亦可依靠專業的一站式管理服務及先進技術，迎接網絡罪案所帶來的挑戰。專業的網絡保安服務供應商憑藉多種技術和對各行各業的深入了解，可為企業度身制定高智能及高度安全的網絡環境，問題將迎刃而解。

戰勝網絡犯罪　WTT有良方

因預料業界對資訊安全服務的需求將激增，WTT因時制宜推出了Asure　Security資訊保安管理服務，為企業抵禦網絡攻擊。作為一家全方位的資訊保安管理服務供應商（MSSP），WTT的資訊安全監控中心（SOC）提供一系列網絡資訊保安管理服務，而且還為企業提供法規遵循顧問服務，為客戶建立資訊保安管理的長遠策略。至今，WTT已為金融服務、醫療保健、物流、零售及旅遊等多個行業的公司加強網絡保安管理，並協助這些企業遵守最新的監管規定。

馬先生認為，提供網絡安全服務是一項持續不斷及靈活萬變的業務，需根據客戶公司的規模、數碼化程度、網絡複雜性及雲端應用等諸多因素，而制定不同的對策。有見及此，WTT採用了能靈活度身訂造、易於啟用的Asure　Security服務組合套裝模式，以滿足企業對資訊保安策略的需求，及配合嚴謹的法規要求。Asure　Security提供24小時全天候監控，配合頂尖UTM防火牆和先進的威脅預防（ATP）技術，築起能主動出

WTT's professional teams provide comprehensive and reliable information security services with a well-managed 24/7 Security Operations Centre (SOC).

in the communities where they do business. The emergence of cybercrimes apparently breaches the order and civilization of the cyber community and causes economic and social disturbance, thus is an issue that a responsible corporate citizen should be eager to address.

As an AWS Advanced Consulting Partner, WTT aims to create a secure cloud environment for its customers when offering its professional and reliable AWS Cloud Enablement Services.

While the general public, or the customers, do not necessarily possess the profound knowledge to stay immune to cyber-attacks, service providers with advanced threat-prevention technologies are unequivocally committed to protecting customers' most valuable digital assets and establishing the strongest first line of defense, by meticulously developing the security functions of their products and services. This is part of WTT's innovative attitude to Corporate Social Responsibility, based not only on sustainable development of the surroundings, but also business ethics and responsible management on the issue of cybersecurity.

WTT believes that cybersecurity is an effort to protect all customers, staff and stakeholders with their best cybersecurity practices and policies supported by their best-of-breed infrastructure. As a key telecommunications operator in Hong Kong, WTT assumes the important role of promoting cyber peace and being the entrepreneurial norm for cybersecurity practices, by providing professional security services and catalyzing positive network effects that contributes to the overall corporate and societal sustainability.

Best Practice for Preventing Cybercrime

Ma notes that the best practice of cybersecurity lies on rational knowledge of risks and discipline of management. In fact, most of the unsophisticated cyber-attacks can be avoided by achieving IT baseline protection management. The real challenge of cybersecurity is protecting mission-critical system against sophisticated attacks. Selecting a right cybersecurity solution partner can provide a comprehensive and professional solution to safeguard the business. ▌▌

擊防禦的第一道堅實防線；清晰明確的安全訊息和事件管理（SIEM）流程能迅速收集保安數據、將多個來源的威脅情報作強大及相互關連的分析，加上擴大識別惡意軟件範圍，令Asure Security各方面都超越傳統的SIEM網絡保安方案。

WTT的網絡安全團隊掌握廣泛的網絡安全技術，對不同企業的關鍵任務需求有深入了解，對嚴格監管環境下運作的金融機構的網絡安全需要具豐富經驗。WTT掌握數碼保安技術趨勢，能有效協助企業應對任何潛在的網絡攻擊，是企業值得信賴的網絡安全合作夥伴。

網絡安全和企業社會責任

未來的商業世界將是一個完全數碼化、互聯互通的世界；於這大趨勢下，沒有周全的網絡安全措施來管理和保護企業的數據的話，企業將要承受數據過度披露、遭惡意利用的風險。

WTT堅信企業社會責任（CSR）與商業目標可以共存，希望透過創新思維來創造更高的商業價值，並在他們從事商業活動的社區中為經濟、社會和環境的可持續發展付出努力。網絡罪案明顯破壞了網絡社會的秩序和文明，引發了經濟和社會的動盪，負責任的企業公民應挺身而出解決問題。

公眾或客戶所擁有的知識未必足以免疫於所有網絡攻擊，因此擁有先進威脅防預技術的服務供應商，絕對有責任為旗下產品和服務提供一絲不苟的防禦保安功能，建立最強的第一道防線，致力保護客戶最有價值的數碼資產。WTT的企業社會責任秉承創新的思維，除致力建構環境的可持續發展外，於維護網絡安全方面，亦採取非常負責任的態度。

WTT相信利用其優質的自建網絡基礎設施，再配合嚴謹制定的安全措施和政策，定能有效保護所有客戶、員工及持份者的利益。作為香港主要的電訊營運商，WTT於網絡和平方面扮演著非常重要的角色，為網絡安全措施樹立企業標準，旨在激發正面的網絡效應，致力推動企業和社會整體的可持續發展。

預防網絡犯罪的最好措施

馬先生指出，應對網絡安全風險的最佳辦法，在於理性認識風險和有紀律的管理。事實上，大多數不成熟的網絡攻擊都可透過IT基線保護管理來避免。網絡安全的真正挑戰是保護關鍵任務系統免受惡意攻擊。透過專業合適的網絡安全解決方案專家為企業制訂全面及專業的網絡安全解決方案，可有效保障企業的數據資產及業務。 ▌▌