A Social Psychological Analysis of the Phenomenon of Underreporting Cybercrimes and the Concomitant Underlying Factors: Three Real Local Case Studies

從社會心理學角度分析網絡罪案的漏報現象及潛在因素：三個本地真實個案研究

Professor Cecilia Cheng, The University of Hong Kong
Mr. Chor-Lam Chau, University College London
Mr. Linus Chan, University of Montana

鄭思雅教授 — 香港大學
鄒楚林先生 — 倫敦大學學院
陳賢諾先生 — 蒙大拿大學

The study was sponsored by the University of Hong Kong Knowledge Exchange Fund. Special thanks are given to researchers Qiu Fangqian and Tu Wenjie of the University of Hong Kong and Hua Zihui, a translator at Tsinghua University.

本研究由香港大學知識交流基金資助。特別鳴謝香港大學研究員邱方倩與屠文潔，及清華大學翻譯員華子慧。

The Prevalent Underreporting of Cybercrime

In the current digital age, cybercrime has become a novel modus operandi to commit crimes and has become a serious problem in society. According to Cybersecurity Ventures' Official 2017 Annual Cybercrime Report (Morgan, 2017), cybercrime is the greatest contemporaneous threat to every company in the world. Last year, Cybersecurity Ventures predicted that cybercrime will cost the world US$6 trillion annually by 2021, up from US$3 trillion in 2015. The negative effects of cybercrime include damage and destruction of data, illegal transfer of funds, decreased productivity, theft of personal and financial data, and theft of intellectual property. The "Current state of cybercrime" published by RSA in 2018 indicated that organizations are challenged on many fronts in their efforts to protect their customers and their businesses against fraud (RSA, 2018).

The increasing popularity of mobile applications for retail, banking and other services makes businesses especially vulnerable to cybercriminals. Therefore, it becomes a prerequisite for organizations to adopt effective approaches to security across all digital channels. The cybercriminals becomes increasingly accustomed and has adapted to different internet platforms, extending from traditional social media channels to more specialized network infrastructure. Furthermore, cybercriminals are developing new tools coeval with advancements in payment services, serving as expedient means to obtain benefits from the

網絡罪案的普遍性和漏報現象

網絡罪案是當今數碼時代的一個新穎的犯案手法，並已經成為社會上的一個嚴重問題。根據2017年發表的「官方年度網絡罪案報告」（Morgan，2017），網絡罪案是現今世界上每家公司所面對最大的威脅。網絡安全風險投資公司預測，到2021年，網絡罪案每年將耗資6萬億美元，遠高於2015年的3萬億美元。網絡罪案帶來的負面影響包括損壞和破壞數據，資金被非法轉移，生產力喪失，個人和財務數據被竊取以及知識產權被盜用。RSA於2018年發表的「網絡罪案現狀」還指出，商業組織在許多方面仍然面臨著保護其客戶和企業免受詐騙的挑戰（RSA，2018）。

移動通信在零售銀行業務和其他服務中的日益普及，使其特別容易受到網絡犯罪分子攻擊，因此商業組織需要確保所有數碼渠道的安全有效方法。而網絡犯罪分子的犯案手法亦日趨老練，並已適應了更多新的網上平台，從傳統的社交媒體渠道延伸到更專業化的網絡基礎設施。再者，由於支付服務的進步和迅速發展，網絡犯罪分子能夠不斷開發新的工具從受害者身上獲取利益。為了應對這種湛新的犯案現象，打擊網絡犯罪活動需要擴展到移動和雲端環境的防欺詐方法。

victims. In order to cope with the new criminal phenomenon, the anti-fraud measures for combating cybercrimes need to be extended to mobile and cloud environments.

The recent loophole of government-developed malware and hoarded vulnerabilities has reflected the constantly developing capabilities of cybercriminals. In addition, the widespread use of new technologies for the Internet of Things (IoT) applications constitutes new vulnerabilities. At the corporate level, the perceived importance of allocating resources for Cybersecurity is accentuated. The 2017 U.S. State of Cybercrime report conducted by CSO revealed that although the average number of security events decreased year-over-year, events that resulted in a loss or damage rose and very few companies reported no losses (Nadeau, 2017). Of the 510 respondents, the number of security events at their company decreased by 8.2% in the past 12 months, from an average of 161 to 148 incidents. More importantly, despite the drop in the number of events, more than two-third (68%) reported that their losses were equivalent or higher than the previous year. The number of businesses that declared to have experienced no losses dropped from 36 percent to 30 percent.

With the development in information technology, Cybercrime perpetrations are coetaneously becoming more mature and normative. However, its reporting rate is lower than that of conventional (offline) crimes. The underreporting of cybercrime is a long-standing problem (McMurdie, 2016; Whitty & Buchanan, 2012). One of the main underlying causes of this phenomenon is that victims of cybercrime are often reluctant to report these crimes. In the business sector, many companies regard the reporting of cybercrimes pertains to the incompetence of their management team or department for data protection. This will instigate negative reports from the media and even attract public, stakeholders' or customers' attention or criticism. Some studies have found that only a disproportionately small proportion of (17%) companies reported losses inflicted by cybercrime (Clough, 2011; Kshetri, 2006). According to a study published by Hildick-Smith in 2005 on underreported cybercrimes, the empirical results clearly support this view. According to the FBI and the Computer Security Institute's estimates, the phenomenon of underreporting of cybercrime incidents in 2002 was quite common, especially in the business sector.

Social Psychological Factors of Underreporting of Cybercrime

The social-psychological phenomenon of underreporting of cybercrime can be explained by the interaction psychological model (Kshetri, 2006; see Figure 1). This model illustrates the interrelationship between the pertinent characteristics of law enforcement, cybercrime victims and cybercriminals. As shown in Figure 1 (the vicious circle), an important factor leading to low reporting rate is the inability of law enforcement agencies to solve cybercrime cases and/or the law enforcement agencies is subjectively perceived to be incapable of solving cybercrimes cases

最近傳媒披露了一些由政府開發的惡意軟件和庇護漏洞的資訊，反映網絡犯罪分子的犯案能力日漸增強。此外，諸如物聯網（Internet of Things/IoT）等新技術的廣泛採用亦會構成新的漏洞。在企業層面上，於網絡安全方面所動用的資源越來越受重視。在2017年 CSO進行的「美國網絡罪案調查」顯示，網絡安全事件的平均數量雖然逐年下降，然而這些事件導致損失的案例卻日益增加，只有極少數公司報告並沒有遭遇任何損失（Nadeau，2017）。在510名受訪者中，他們的公司受網絡安全所影響之事件數量，在過去一年中從平均161件下降至148件，下降了8.2％；但值得注意的是，儘管受網絡安全所影響的事件數量下降，但有超過三分之二 (68％)的受訪者表示，他們的公司遭受之損失卻與前一年相同或更高。聲稱沒有遭受任何虧損的公司數量也從36％下降到30％。

隨著信息技術的發展越來越先進，網絡罪案亦日趨成熟及普遍，但其報案率卻相較傳統（離線）犯罪之報案率為低。罪案漏報問題由來已久（McMurdie，2016；Whitty & Buchanan，2012），造成這現象長期存在的一個主要的潛在原因，是網絡罪案的受害者往往並不願意舉報這些罪行。例如在商界，很多公司對舉報網絡罪行一事通常會視作其管理團隊或部門在數據保護方面不稱職，擔憂舉報網絡罪行後，會帶來傳媒的負面報道，甚至招致公眾或客戶群的關注或批評。一些研究統計發現，只有不成比例的極少部分（17%）公司舉報了因為網絡罪案所造成的損失（Clough，2011；Kshetri，2006）。根據Hildick-Smith在2005年發表關於漏報網絡罪案的研究，實證結果亦明確支持了這觀點。根據聯邦調查局和電腦安全研究所對網絡罪案數量的推斷，表明2002年間的網絡罪案事件漏報現象亦相當普遍，尤其是在商界發生的網絡罪案極為嚴重。

漏報網絡罪案的社會心理因素

漏報網絡罪案這種社會心理現象可以用交互心理模型（Kshetri, 2006；見附圖1）所解釋。這個模型說明執法部門、網絡罪案受害者和網絡犯罪分子三者特點之間的相互關係。如圖1（惡性循環）所展示，一個導致低報案率的重要因素是執法部門沒有足夠能力破案，又或是執法部門被網絡罪案受害者或網絡犯罪分子主觀認為是沒有足夠能力破案。關於執法部門被質疑沒有能力跟上當前的網絡犯罪技術，缺乏處理網絡罪案的經驗以及無法有效地解決網絡罪案的普遍認知（又或是反映實際情況）造成了嚴重的後果（Clough, 2011）。這引起網絡罪案受害者對執法部門（例如警察和聯邦調查局）的信心下降，導

by cybercrime victims or cybercriminals. The law enforcement agencies have been questioned about the inability to catch up with current cybercrime technologies, inexperience in dealing with cybercrimes and the inefficient in addressing the widespread beliefs revolving around cybercrime (and/or beliefs reflective of the actual conditions) led to serious repercussions (Clough, 2011). This reduces cybercrime victims confidence in law enforcement agencies (Such as Police forces and FBI); inadvertently adhering to the interests of cybercriminals. Consequently, the cybercriminal will have more experiences of success, accompanied by the enhancement of confidence in their criminal behaviors (Kshetri, 2006).

In addition, the difficulties of detecting, tracking and tracing cybercriminals, as well as the aforementioned predicaments contended by law enforcements, will pose more problems for law enforcement agencies in tackling cybercrime. Therefore, the processes of investigating and reporting cybercrime often become more difficult and discouraging. Even if these cybercrimes are reported, many countries (especially those with underdeveloped economies and lack of resources) will not investigate all cybercrimes because the cybercrime investigation process is extremely complex, expertise-intensive, resource-intensive, and cost-intensive. For instance, a study revealed that only 15 percent of all reported cybercrimes were investigated by law enforcement agencies, and the rate of detection was not high (Kshetri, 2006).

By comparing the characteristics of cybercrime and conventional (offline) crime, it was identified by some studies that there was no conspicuous difference between the two types of criminals; such as involvement of collusions as groups with organizational structure and specialization (Broadhurst et. al, 2014); having similar means, or "similarities between traditional crime techniques and cybercrime techniques" (Sinca, 2015, p. 63). Though this remain to be a contested territory, where other studies such as that by indicated otherwise (Nykodym, Taylor & Vilela, 2005); in Russia, for instance, most of the hackers are higher educated, young and work independently and they do not possess conventional criminal characteristics (Kshetri, 2006).

The development of information and communication technologies facilitated the extensive communication and cooperation between different countries (including criminal activities and cybercrime). With the globalization of cybercrime and the anonymity of cybercriminals, cybercriminals can extend their criminal behavior beyond their location and/or country (Kshetri, 2006; Wall, 2001). Therefore, most of the investigations of cybercrime would face legal issues (Teng, 2017). In large scale investigations, trans-national cybercrimes would often incur more time. For instance, in 2000, the United States arrested two Russian hackers by luring them to the US with job offers. They downloaded data from the hackers' computers. Then, these hackers were prosecuted despite that Russia claimed that the FBI was illegally (referring to hacking behavior) downloaded data from computers located in Russia. According to the vicious circle of cybercrime by Kshetri (2006)

致報案率低，無意間正中了網絡犯罪分子下懷。因此，網絡犯罪分子將擁有更多的成功經驗和隨之而來對其犯罪行為的自信（Kshetri, 2006）。

此外，偵查、追蹤和追查網絡犯罪分子的困難，以及所涉及到的執法困難亦會給執法部門在破解網絡罪案方面構成了更多的問題；因此調查和通報網絡罪案的過程往往變得更加困難和令人沮喪。即使這些網絡罪案被舉報了，因為網絡罪案的調查過程是異常複雜、專業知識密集型、資源密集型以及成本密集型的，所以很多國家（尤其是經濟不發達而資源缺乏的國）並不會調查所有網絡罪案。例如，研究發現在所有的被舉報的網絡罪案中，僅有百分之十五會被執法部門立案調查，而且當中破案率並不高（Kshetri，2006）。

通過對網絡罪案和傳統（離線）罪案特徵之間的比較，一些研究發現這兩類犯罪分子之間並沒有顯著的差異；例如將共謀作為具有組織結構和專業化的群體（Broadhurst et. al，2014）；具有類似手段，或"傳統犯罪技術與網絡犯罪技術之間的相似性"（Sinca，2015，p.63）。但這仍然是一個有爭議的領域，其他研究有不同的發現（Nykodym，Taylor & Vilela，2005）。執法部門缺乏網絡罪案數據庫，進一步阻礙了預測和解決網絡罪案。例如，俄羅斯大部分黑客是受過高等教育的、年輕的和工作獨立的，他們並不符合傳統罪案犯罪分子的特徵（Kshetri，2006）。

信息和通信技術的發展促進了不同國家之間更為廣泛的相互通訊與合作（包括犯罪活動和網絡罪案）。隨著網絡罪案的全球化和網絡犯罪分子的匿名性，網絡犯罪分子可以將他們的犯罪行為擴展到他們所在的國家之外（Kshetri，2006；Wall，2001）。因此，很大部分對網絡罪案的調查將會面臨法律問題（Teng，2017）。在大型調查中，跨國的網絡罪案往往需要更多的時間來應對，並會招致更大的法律糾紛。例如，2000年美國誘使2名黑客工作，並逮捕了他們。根據從俄羅斯黑客電腦中下載的信息，這些黑客受到了檢控。儘管在2002年，俄羅斯聲稱美國聯邦調查局實施了從俄羅斯電腦上下載數據的非法活動（黑客行為）。根據Kshetri（2006）的模型所提出的網絡罪案的惡性循環，這些問題甚至是解決網絡罪案問題的失敗導致了網絡罪案受害者對執法部門信心的下降，因此這些受害者更加不願意舉報網絡犯罪行為。

model, these problems and even the failure to solve cybercrime problems led to the reduction in cybercrime victims' confidence in law enforcement agencies. The complex composition of these factors constituted the cybercrime victim's unwillingness to report cybercrime.

Overview of Hong Kong Telephone Scam Case Studies

In Hong Kong, there is lack of cybercrime analysis for businesses. But, the coetaneous prevailing Hong Kong telephone scams were targeted on new immigrants and visitors. According to Mr. Lee Ka Chiu John - Secretary for Security, the number of cases related to telephone scam had decreased in 2017, but the financial losses had increased (Leung, South China Morning Post, 2017a). According to Counterfeit, Forgery and Support Division of Commercial Crime Bureau disclosed that most of the victims were new immigrants and visitors coming from mainland China. There were 426 confirmed cases of telephone deception in the first three quarters and more than one-third of the victims were mainland Chinese university students (Leung, South China Morning Post, 2017b). They have suffered various degrees of financial losses ranging from ten thousands of Hong Kong dollars to hundreds of thousands or even millions of Hong Kong dollars.

According to Superintendent Chan Tin Chu Andy - Counterfeit, Forgery And Support Division of Commercial Crime Bureau said that the telephone scammers are inclined to impersonate immigration officers, using "Official Documents" to lure the victims because these "Official Documents" are very important for new immigrants. Hence, the new immigrants from mainland China may be affected by the psychological disconcertion and become more susceptible to deception (Leung, 2017b). These concerns and face-saving culture of Chinese often led to the problem of underreporting of crimes aforementioned. Thus, these reported telephone deception cases are only the tip of the iceberg.

In order to further investigate the cybercrime victims' psychological status and thereby helping the new immigrants from mainland China to prevent from being deceived from this type of fraud, the Social and Health Psychology Laboratory of the Department of Psychology at the University of Hong Kong conducted an academic research from February to April in 2018 to further understand the modus operandi and characteristics of this type of scams. The research was conducted via several internet platforms such as Weibo and WeChat. A total of 80 mainland students were recruited to participants of this study. Nearly 90% of the respondents have heard of mainland students tricked by telephone, and 70% of the respondents have received suspicious deception calls. This illustrates that telephone scam is often targeting the group studied. It is most noteworthy and concerning that 5% of the respondents admitted that they have suffered financial loss in telephone deception. But, when the research team invited those victims to participate in a further interview of greater depth, none of them were willing to participate.

本地電話詐騙的個案研究概觀

在本港，有關商界發生的網絡罪案之相關研究甚為缺乏；但近年來本港普遍存在電話詐騙案件，本港警方對新來港人士或訪客所遭電話詐騙案件甚為關注。根據香港特別行政區政府保安局局長李家超透露，2017年電話詐騙案數量雖然有所減少，但財務損失數字卻恰好相反（Leung，南華早報，2017a）。根據本港警方商業罪案調查科偽鈔及偽造文件組透露，這些電話詐騙案件的大部分受害者均是來自中國大陸的新來港人士或訪客，在2017年年前三個季度，電話詐騙案件多達426宗，其中三分之一以上是大陸新來港的大學生（Leung，南華早報，2017b）。這些新來港學生遭受了不同程度的經濟損失，受騙金額少則幾萬港元，多則幾十萬甚至幾百萬港元。

本港警方商業罪案調查科偽鈔及偽造文件組警司陳天柱表示，由於網絡犯罪分子傾向擔任偽冒入境處官員，並使用入境”官方文件”作為誘餌，因為這些”官方文件”對大陸新來港人士來說非常重要，所以大陸新來港人士之所以容易被網絡犯罪分子欺騙是因為心理上的擔憂（Leung，2017b）。這些擔憂及中國人普遍的顧全面子心理往往導致較早前所述的罪案漏報問題，因此這些電話詐騙案件數字極可能只是冰山一角。

為了更詳細研究網絡罪案受害者的心理狀態，從而更好地幫助大陸新來港人士預防此類詐騙，香港大學社會及健康心理學實驗室於2018年二月至四月進行了一項學術研究，以深入了解此類詐騙的手法及特徵。此研究在網上、微博和微信多個平台上進行，其間一共收集了八十個大陸留港學生的樣本。當中近九成受訪者有聽説過大陸留港人士遭遇電話詐騙，並有七成受訪者收過疑似詐騙的電話，顯示電話詐騙於這個群組相當普遍。更值得關注的是，有百分之五的受訪者承認自己在電話詐騙遭遇過經濟損失，但當本研究團隊邀請這些網絡罪案受害者參與一個後續深入訪談，卻並無任何一位遭遇過經濟損失的受害者願意參與此訪談。

本研究團隊繼而邀請另一群收過疑似詐騙電話但未有遭遇任何經濟損失的受訪者參與這個後續深入訪談。當中原有八位受訪者答應參與，但預約好訪談當日卻只有三位受訪者應約參與。這三位受訪者（或轉述的當事人）全是能夠避免在詐騙過程上當的成功個案，他們在訪談中所產生的寶貴數據，可作為預防大陸新來港人士免遭電話詐騙的最佳實踐指南。我們在以下部分描述與這三個成功個案的訪談結果。

The research team invited another group of respondents (who had received suspicious scam calls but whom did not suffer any financial loss) to participate a further interview. Originally, eight respondents agreed to attend the interview; though, only three of them participated. From these three respondents (or the paraphrasing parties), all of them successfully avoided losses in telephone deception. We obtained valuable information from them and generated strategies to prevent losses from telephone scams. The following described the interview results of three successful cases:

The Best Practice Guideline for Preventing Telephone Scam Victimization

Case 1

The first respondent's information serves as a primary source, as he received the call from telephone scammer (caller) who pretended to help the respondent in handling and investigating suspicious parcels found by the Custom and Exercise Department, and to lure him to disclose his personal information. The respondent did not fulfilled the scammer's request. Instead, he asked the scammer for background information (such as the name of courier company, the full name of the receiver and the telephone number) in order to verify whether the scammer's request was rational. Although the scammer tried not to reply directly the respondent's questions by repeatedly affirming attempting to help out of kindness, this elicited suspicion of the identity of the caller.

Although respondent 1 was initially stressed, he was not overwhelmed by this nor victimized. This can be ascribed to the increasingly noticeable (four dimensions of) suspiciousness of the caller, this refers to 1) the caller only knew the surname of the respondent rather than the full name, 2) the parcel did not exist, 3) the caller's tone of voice appeared to be exceedingly convivial and 4) judgment of caller being highly unlikely to be originating from Hong Kong because of his mainland Chinese accent. After hanging up the phone, the respondent thought critically about the conversation and realized that this was a telephone scam. Such a conclusion is drawn based on memory cueing, which involved thinking about his friend having a similar experience with telephone scam (of the scams having similar characteristics) and he had also heard about the risk of telephone scams previously.

The respondent noticed that the scam might be more effective if the scammer forced him to call another phone number. In this way, the potential victim will seem to be more involved with the case because they take the initiative to make the call.

As a precautionary initiative against telephone fraud, the respondent suggested that we should share own-experience to friends, even to schools and the police department. The attempt of deception was unsuccessful because the respondent did not follow the scammer's instructions. Respondent 1 showed some form of defensive attitude (a form of defence mechanism stated in the model), has some understanding and awareness of telephone fraud. These factors can reduce the chances of success

本地電話詐騙的最佳實踐指南

個案一

第一位受訪者以當事人身份告訴訪談人員，電話詐騙犯罪分子（來電者）要求當事人提供個人資料，來電者偽裝成能夠幫助當事人追查海關發現的可疑包裹。當事人沒有立即答覆，並要求來電者提供一些背景資料（即速遞公司名稱，收件人全名及電話號碼），以確定其要求的合理性。因為來電者反覆向當事人保證自己是出於善意幫助，嘗試去避免回答這些問題，所以當事人開始對來電者產生了懷疑。

儘管當事人最初感到緊張，但他並沒有因此而陷入騙局，因為隨著與來電者電話對話的進展，疑點越來越明顯，也就是說1）來電者只知當事人的姓氏而非全名，2）這個包裹根本不存在，3）來電者的語氣聽起來太體貼，4）來電者有大陸口音，因此來電者極有可能不是來自香港。通話結束後，當事人一再細心思考該電話的對話內容，並意識到這確實是詐騙電話，因為當事人想起有朋友也經歷過相似特徵的欺詐性電話，而當事人以前亦已聽聞有關電話詐騙的風險。

當事人注意到為使電話詐騙更有效，來電者應該強迫當事人主動緊急地去撥打另一個電話。這樣一來，當事人就會感受到更加投入，因為是自己主動撥打的。

為了倡議對電話欺騙案件的警惕，當事人建議與身邊的人， 甚至學校和警察機構分享自己的經歷。這個案並不成功，因為當事人沒有立即聽從電話詐騙犯罪分子的指令，顯示了一些防禦態度，並且有一些電話詐騙案件的認知。這些因素減少電話欺騙案件的成功機會,所以我們早前提出的理論模型得以支持。

個案二

第二位受訪者沒有親身經歷電話騙案，而是轉述了一位朋友（當事人）的經歷。這電話詐騙犯罪分子（來電者）是一位聲稱來自上海的財務機構人員，並負責管理大陸留港學生的資金；來電者要求當事人提供銀行賬戶資料。剛巧當事人正遇到銀行帳戶驗證問題，所以當事人立即告訴了來電者一些重要個人信息，甚至信用卡的三位驗證碼。幸運地，這騙局最終失敗了，因為當事人在透露這些私人信息後感到驚慌失措，並在翌日選擇凍結自己的銀行賬戶。

受訪者認為，令電話詐騙案件之所以有成效，犯罪分子應該早

of telephone fraud, serving as corroborative support for our proposed model.

Case 2

The second respondent did not directly experience telephone fraud, but shared his friend's experience. The scammer (caller) claimed to be a financial officer from Shanghai, who is responsible for managing the funds of mainland students in Hong Kong. Subsequently, the scammer requested information for his friend's bank account information. The friend happened to experience problems with his bank account verification procedures, so he told the scammer some important information, including a credit card's three-digit verification code. Fortunately, the scam failed because his friend was apprehensive after disclosing this information and requested to freeze his bank account next day.

Respondent 2 believes that for cybercrimes to be effective, scammers should already know some information about the target for fraud. They should also know that the targeted individual wants to verify the information. In addition, scammers could create fraudulent bureaucracy where scam calls are transferred to different contrived "departments".

This case elucidated that to combat telephone fraud, individuals who received such calls should remain calm, vigilant and refuse to give information to the caller until the caller's identity is verified. An example of an indicator for potential danger would be a caller from Shanghai should have a mainland accent but not a Hong Kong accent.

Respondent 2 believes that augmenting public awareness is to the prerequisite for reducing cybercrime. The Hong Kong police could inform citizens that they never ask for identifiable information through phone calls and cooperate with schools to disseminate the message. Schools could inform the students about cybercrime by providing reference materials such as booklets through email.

Although the respondent complied with the scammer's request for financial information, he displayed a form of defence mechanism (i.e., freezing bank account) which prevented the scammer's success. Thus, this case study contributes to supporting evidence that supports our proposed model.

Case 3

The third respondent is directly involved in the call. He answered a phone call that began with voice recordings (which was thought to be an organization's personnel by respondent 3) followed by the scammer's voice pretending to be an official of a government authority. The scammer threatened respondent 3 for money in a very urgent tone. Respondent 3 requested scammer to explain the procedures involved to solve the problem. The pre-recordings of threats pertinent to legal repercussions (if directions were not followed) were usually presented with a female voice.

已知道一些關於當事人的信息，並且知道他們需要驗證信息。此外，犯罪分子可能會設立一個假的機構架構，將電話轉駁到不同部門來建立權威。

這個案説明為了防止電話詐騙案件，當事人們應該保持冷靜，保持警覺，並拒絕向來電者提供私人資料，直至來電者身份被證實。受訪者舉一個簡單例子：如來自上海的來電者應該有大陸口音而不是香港口音。

受訪者認為，需要加強宣傳從而減少網絡罪行。香港警方可以通知市民，他們從來不會以電話要求提供身份確認信息，並可與學校合作傳播此信息。學校可以透過電子郵件向每個學生發送有關網絡罪行的小冊子。

雖然當事人遵從詐騙者的財務信息要求，但當事人亦展示了防止詐騙者成功的防禦策略（即凍結銀行賬戶）。因此，這個案例也支持我們提出的理論模型。

個案三

第三位受訪者以當事人身份接受訪問，透露起初接聽到一個偽裝是某機構人員的電話錄音。這位來電者以非常緊急的語氣威脅當事人索取金錢。而當事人亦向來電者查問程序去解決事情。如果當事人不遵循指示，通常被威脅會引起法律後果，而這預設錄音通常都是由女性聲音錄製的。

當事人知道有很多電話詐騙案件，並且知道該電話從一開始就是詐騙性的。當事人非常清楚近幾年發生過的電話詐騙案件。因此，當事人不信任這未知來電者的電話。

與個案一和個案二相似，這位當事人指出，令網絡罪行之所以有成效，電話詐騙犯罪分子應該早已經知道一些關於當事人的信息，當事人們應該通過其他渠道確認來電者是否真實。最後當事人認為增加宣傳會減少電話騙案。

這個案例再次支持我們提出的理論模型，因為對電話詐騙案件的先驗知識導致受訪者對犯罪分子來電持謹慎態度，這些先驗知識保護了當事人免受威脅和恐嚇。

Respondent 3 is well aware of the telephone fraud cases for the recent years, and he was astutely aware that the call was deceptive. Therefore, respondent 3 will not to trust any unknown callers.

Similar to cases 1 and 2, this respondent noted a constituent element for cybercrimes' successes, which is scammers' pre-existing knowledge of background information about the victims. The victim should confirm if the caller is authentic through other channels. He believes that more widespread dissemination of issues relating to cybercrimes will help to reduce telephone fraud cases.

This case again supports our proposed model, because prior knowledge of fraudulent calls led the potential victim to be cautious of fraudulent callers. This prior knowledge protected the respondents from threats and intimidation.

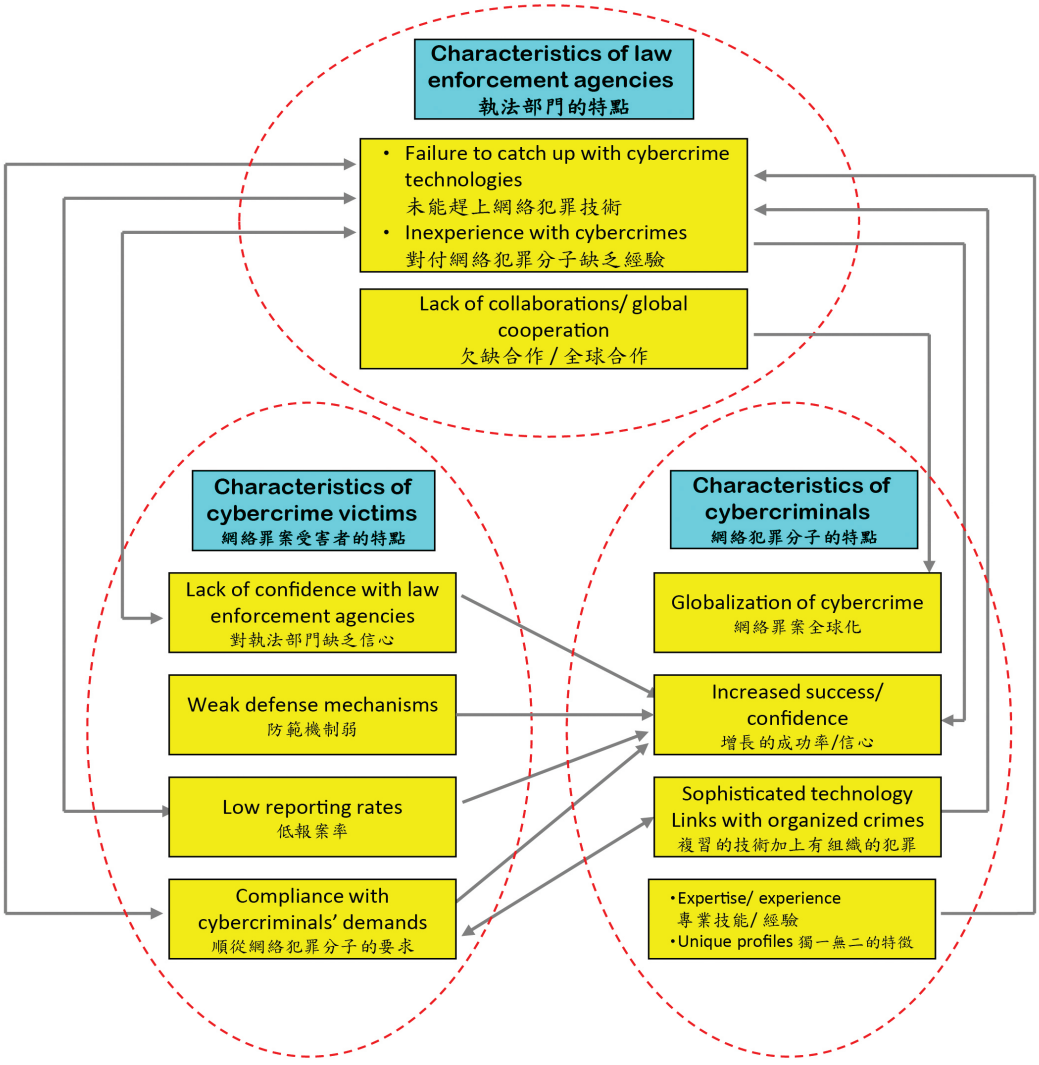

Figure 1 : The vicious circle of cybercrimes. The proposed framework outlines how the characteristics of law enforcement agencies, cybercrime victims and cybercriminals are inextricably intertwined, and shaped the cybercrime phenomenon.

圖1： 網絡罪案的惡性循環。擬議的框架概述了執法部門、網絡罪案受害者和網絡犯罪分子的特點是如何塑造網絡罪案的現象。

References
參考文獻

Broadhurst, R., Grabosky, P., Alazab, M., Bouhours, B., & Chon, S. (2014). An analysis of the nature of groups engaged in cyber crime. Nykodym, N., Taylor, R., & Vilela, J. (2005). Criminal profiling and insider cyber crime. Computer Law & Security Review, 21(5), 408-414.

Clough I. J. (2011). Cybercrime. Commonwealth Law Bulletin, 37, 671-680.

Hildick-Smith, A. (2005). Security for critical infrastructure SCADA systems. SANS Reading Room, GSEC Practical Assignment (Ver. 1), 498-506.

Kshetri, N. (2006). The simple economics of cybercrimes. IEEE Security and Privacy, 4, 33-39.

Leung, C. (2017a, October 24). Here are the two key reasons people keep falling for phone scams in Hong Kong. South China Morning Post. Retrieved from http://www.scmp.com/news/hong-kong/law-crime/article/2116610/here-are-two-key-reasons-people-keep-falling-phone-scams

Leung, C. (2017b, November 28). Hong Kong university student loses HK$220,000 in phone scam. South China Morning Post. Retrieved from http://www.scmp.com/news/hong-kong/law-crime/article/2121855/hong-kong-university-student-18-loses-hk200000-phone-scam

McMurdie, C. (2016). The cybercrime landscape and our policing response. Journal of Cyber Policy, 1, 85-93.

Morgan, S. (2017). 2017 Official Annual Cybercrime Report. Cybersecurity Ventures.

Nadeau, M. (2017). 2017 U.S. State of Cybercrime survey. CSO.

Nykodym, N., Taylor, R., & Vilela, J. (2005). Criminal profiling and insider cyber crime. Computer Law & Security Review, 21(5), 408-414.

RSA. (2018). 2018 Current State of Cybercrime. RSA.

Sinca, G. M. (2015). Cybercriminology: Transition from Traditional Criminal Techniques to Cybercrime. AGORA International Journal of Juridical Sciences, 62-66.

Teng, A. (2017). Jurisdictional Barriers: Cybercrime Prosecution Challenges (Unpublished Doctoral dissertation, Utica College, New York, NY).

Wall, D. (2001). Cybercrimes and the Internet. In D.S. Wall (Ed.), Crime and the Internet (p. 1-17). New York, NY: Routledge.

Whitty, M. T., & Buchanan, T. (2012). The online romance scam: A serious cybercrime. CyberPsychology, Behavior, and Social Networking, 15, 181-183.