

ATM Heist Threats: A Proposed ICT Governance Strategy

Da-Yu KAO

Department of Information Management, Central Police University, Taiwan

camel@mail.cpu.edu.tw

Abstract—Cyber black markets for hacking tools or services are gaining widespread attention as more advanced persistent threat attacks are relevant to such markets. In July 2016, the ATM heist of Taiwan First bank is based on well-known Carberp malware family, which is available for sharing, sale or cooperation on such markets. This study reviews organizational cybercrime activities and ATM threats, and proposes an ICT governance framework in online ATM heist management. This framework further points out capable people, efficient process, effective technology, and data governance. This framework is potentially useful for cybercrime prevention.

Keywords—cybercrime, ATM threat, bank malware, criminal group, financial technology

I. INTRODUCTION

A. Sophisticated ICT environment

The Internet has become an integral part of our society and it enriches our lives in countless ways. Information and communications technologies (ICTs) are the integration of telecommunications, computers and software, which enable users to access, store, transmit, and manipulate information. As the computer systems of new ICT environment get more sophisticated, so do the criminals. ICTs have facilitated not only the methods in which crimes are committed but also the methods in which criminals interact in committing them.

B. Financial Technology

Financial Technology (FinTech) refers to the use of software and digital platforms to deliver money exchange services to consumers, and make it easier than ever to make transactions between two entities [16]. While much cybercrime is committed by individuals acting alone, a significant amount is accomplished by criminal groups acting in concert. These groups have tended to vary significantly in their criminal activities in which they engage. Cybercrimes are developing exponentially and threatening our FinTech. To fight against the unlimited growth of ATM security threats, a sound knowledge of the problem and perpetrators can contribute to prevent from cybercrimes.

1) Advantages

a) The Traditional Need for Strict Security Controls

Banks use many electronic systems, including Automated Teller Machines (ATMs), for the operation of their financial environment. Traditionally, they use strict security controls over all operational and transaction-related procedures. In terms of segregation of duties, all systems administration must

have dual login controls, rare network protocols and multiple serial firewalls for internal banking communications [16]. However, banks generally choose open system due to friendly user-interface, convenient process or insufficient budget.

b) Online ATMs for Convenient Payment Activities

Online ATMs have gained increasing popularity all over the world, as they provide convenience to the public in managing their banking accounts and payment activities [16]. The vulnerability of complicated, fragmented ATM system relies on many providers to get customers cash on demand. Due to the growth of FinTech, some ATM services have offered convenient payment solutions to facilitate online internal examination.

2) Disadvantages

a) The Lack of Cybersecurity Awareness

Exploits take advantage of weaknesses or vulnerabilities in software. A vulnerability run malicious code onto compromised computers. Malware can further infect other internal computers without users' knowledge [13]. Financial ATMs to internet-connected industries should simply not be built using commercial operating systems for safety concern. The lack of cybersecurity awareness may enhance the vulnerability of individuals and organizations. The threat of cybercrime impedes the development of information technology. It could contribute to the weakening of a nation's economy security.

b) Unauthorized Access of Internal ATM Details

How can the hacker group obtain the internal ATM information? Internal IP Address, computer name and device name should be difficult to match them. As far as ICT governance is concerned, this kind of data is limited to internal key persons. The main threat arising is the possibility of unauthorized access and use of bank card/ATM information by a fraudster [16].

The literature reviews of organizational cybercrime activities and ATM threats are discussed in Section 2. Section 3 describes USA's Unlimited Operations on prepaid debit accounts and recent ATM threats. Discussions and analyses on ATM malware family are illustrated in Section 4. In Section 5, a proposed ICT governance framework of ATM heist management is discussed into four categories: capable people, efficient process, effective technology, and data governance. Our conclusions are given in Section 6.

II. LITERATURE REVIEWS

A. Organizational Cybercrime Activities

Cybercrime is a rapidly growing phenomenon that requires a proactive and coordinated response. The convenience for a user has become another advantage for criminals [7]. The diversity of organized cybercriminal exploits by state and non-state actors alike. Criminal offenders or nation-states have entailed a diverse set of organizational activities. The following activities in Table 1 describe a number of organizational cybercrime activities in recent years.

B. The Shadowy Criminal Group on ATM Threats

1) Bank Malware Family

Some of the most notable malware families are Zeus (its successor Carberp), and Carberp (its successor Carbanak). The criminal's pragmatic approach starts a new chapter in the cybercrime ecosystem [3, 5]. In this era of increasing cyber-attacks, many different malware families are programmed specifically for the majority of internet banking fraud through malware. Traditional bank heists are becoming large-scale hackers with its unlimited borders, as cybercrime against

financial banks turns out to be an increasingly convenient way to withdraw big money. This study focused on the Carberp malware, and it showed there was a grey area between APT and malware.

2) Shadowy Criminal Group on ATM Threats

There are a variety of shadowy criminal groups that focus on banks and payment providers. The ATM threat has continued to infect ATMs all over the world [10]. An ATM can be hacked even though it is protected by camera videos or other locked vaults. The shadowy criminal group members began actively taking an interest in retail organizations or bank payment systems [5]. Hackers hacked up to \$1 billion from more than 100 banks in 30 countries. ATM hacking is becoming a new trend for an organized cybercrime group. There are certain tutorial, tricks and techniques online about ATM devices hacking like Diebold, Defcon or Wincor Nixdorf [17]. It is not really easy to cheat an ATM computer. If cybercrime targets financial services, it requires advanced hacking capability. Profit or money is always an initial motivation for criminals, who have targeted ATMs to withdraw cash even without the need of a card.

Table 1: Organizational Cybercrime Activities

Year	Group Name	Actor Type	Behavior Type	Activity
1993~2001	DrinkOrDie (DoD)	Non-state	An international group of copyright pirates	Illegally reproduced and distributed software, games, and movies over the Internet.
1996~1998	The Wonderland Club		A members-only group	Exchanged illicit images of children.
2003~	Anonymous		A very loose and decentralized group of activist and hacktivist entities.	Focus on website defacements, distributed denial of service attacks, and prominent symbols
2006~2008	Dark Market		A forum for the exchange of stolen credit card and banking details, malicious software, and related technology.	Take advantage of the criminal opportunities presented by the advent of electronic banking and the increasing use of credit and debit cards.
2006~2010	PLA Unit 61398	State	A large-scale program of industrial espionage	Acquire a massive volume of data from a wide variety of industries in English-speaking countries.
	Shady RAT		An ongoing series of cyber-attacks	Hit at least 71 organizations
	Aurora		A series of cyber-attacks	Aim at dozens of other organizations
	GhostNet		A cyber espionage operation	Operate from commercial Internet accounts in China.
2007~2013	PRISM		A systematic harvesting program of digital information by the US National Security Agency (NSA).	Capture and store a wide range of Internet data on the following prominent IT companies: Microsoft, Google, Yahoo!, Facebook, Pal Talk, YouTube, Skype, AOL, and Apple.
2010	Operation Olympic Games		A collaboration between the US National Security Agency and its Israeli counterpart, Unit 8200.	Disrupt the Iranian nuclear enrichment program.
	Stuxnet		A malicious computer worm (Stuxnet) is believed to be a jointly built American-Israeli cyber weapon	Involve the clandestine insertion of an extremely complex and sophisticated set of software into communications and control systems at the Natanz nuclear facility.
2010~2012	Ukrainian Zeus Group	Non-state	Software engineers in Eastern Europe	Gain access to the computers of individuals employed in a variety of small businesses, municipalities, and non-government organizations in the United States.

III. SAMPLE CASE

A. USA's Unlimited Operations on Prepaid Debit Accounts

The hackers from Unlimited Operations were able to infiltrate various credit card companies and raise withdrawal limits on prepaid accounts from thousands of ATMs in a looting. These cybercrime thefts were based on a sophisticated computer hacking procedure, whereby prepaid debit card information was stolen from the computers of financial banks. By using prepaid debit cards, the criminals were able to avoid the alarms. The cards were then adjusted to have unlimited balances, so that groups of criminals across the world could use the cards to withdraw the maximum amount from the ATMs. The thefts carried out ATM heists in New York, Canada, Mexico, the Dominican Republic, Colombia, the UK, Belgium, France, the Netherlands, Germany, Spain, Italy, Bulgaria, Romania, Latvia, Estonia, Ukraine, Egypt, South Africa, Russia, the United Arab Emirates, Pakistan, Sri Lanka, Russia, Thailand, Malaysia, Indonesia, Japan and so on. Between December 2012 and February 2013, a cyber-group of criminals, operating in more than 24 countries, stole \$45 million from the accounts of financial banks themselves, rather than customer accounts. The cyberattacks employed by the suspects (Elvis Rafael Rodriguez and Emir Yasser Yeje) and their co-conspirators are known as Unlimited Operations in the cyber underworld. Eight suspects were charged in May 2013 for the New York portion of the thefts. The alleged leader of the group, Alberto Yusi Lajud-Peña, was dead in the Dominican Republic on April 27, 2013 [7]. Six of the seven suspects were under 25 years, and all were US citizens. Two worked as bus drivers for a private company [2]. Their criminal scheme involved distributing smaller sums of money across bank accounts, and purchasing expensive luxury items.

B. Recent ATM Threats

In recent years there has been a tremendous increase in organization crimes. Banks in many countries are becoming new targets of several independent Russian cybercrime groups. Traditional organization crimes have a hierarchical top-down command-and-control structure, but cybercrime groups tend to involve a loose network or even a peer-to-peer decentralized structure [16]. The group operated in closed cells, and the suspects did not know each other involved in the ATM heist [15]. These attacks rely upon both highly sophisticated hackers and closed criminal cells whose role is to withdraw the cash as quickly as possible. The crime chain is the series of steps cybercriminals go through to transform its ATM invasion into something of greater value. They make its output worth more than the sum of its inputs. Their activities can be divided into primary activities, the foundation on which this organization rests, and support activities, which span the primary activities [6]. Primary activities differ from one organization crime to another. Activities contribute directly to initiating, committing, collecting, and supporting the crime. Support activities are usually similar in. The ATM transactions in USA's Unlimited Operations require only general bank card information to effect a payment, such as the bank card number, and PIN code. However, Taiwan's Russian

Mafia Group in July 2016 further compromises the ATM systems and criminals can withdraw money without any bank card information.

IV. DISCUSSIONS AND ANALYSES ON ATM MALWARE FAMILY

Increased access to the Internet has enabled cybercriminals to perform reconnaissance on their targets using the surface, deep and dark web to run more successful large-scale fraud attacks. A significant amount of malware targets financial organizations, bypass security tools, and deploys various anti-forensics tricks in an attempt to make analysis more difficult. Cyber threats are still profitable for cybercrime groups and sponsored APT groups, who may attack bank systems for financial profits or political reasons. Cybercrime investigation of these cyber threats through hacker tools, techniques, and procedures is critical for law enforcement agencies to protect users and reduce the fraud risk.

A. Functional Comparison

An organized group of hackers from Russia and Ukraine has broken into internal networks at dozens of financial banks and installed malware that allowed the group to drain bank ATMs of cash. The ATM malware family in Latin America, Europe, and Asia are identified as 'Carberp,' 'Qadars,' 'Ploutus,' 'Tyupkin,' 'Anunak,' or 'Carbanak' during the period from 2009 to 2015 in Table 2. This malware has evolved over time and has added functionality beyond banking credential theft. The details of each malware are somewhat different, and the stealthy APT methods used by the attackers in these heists would work across a broad range of commercial banks one by one. This group specializes in hacking into banks directly, and then working out ingenious ways to funnel cash directly from the financial institution itself [5].

B. Behavioral Comparison

Since 2009, researchers have warned that hackers were developing malicious software for ATMs [1, 4, 14, 18]. Hackers may exploit security flaws in specific ATMs, and cause the compromised machines to spew a flurry of bills onstage. The behavioural comparison of ATM malware family is listed in Table 3. These three cases were arrested by the law enforcement agencies.

C. Proper Security Measures

1) Cybercrime Vendors in Dark Web

In Dark Web, cybercrime vendors sold access to a wide selection of malware or compromised zombies from any country. Price tags for remote desktop-based access run no more than a few dollars. The criminal group could buy access to bank employee computers that were already compromised by massively distributed opportunistic malware [9].

2) A Wide Variety of Malware

The hacker forums offer criminals a wide variety of malware for low prices to assist them in criminal activities. The Carberp malware source code was acquired and enhanced to create new threat product for sale to the underground fraud community [11]. Leaking the source code was like the leaking

of a tank factory. The future damage cannot be limited or controlled. The do-it-yourself malware toolkit sold by the group has been used to make unauthorized banking transactions. The proper security measures for banks are recommended both to the cashpoints and the environment they are placed in, with sufficient lighting and cameras monitoring all activity [5, 8].

- Review the physical security of all ATMs
- Consider investing in quality security solutions.

- Replace all locks and master keys on the upper hood of the ATM machines
- Ditch the defaults provided by the manufacturer.
- Install an alarm and ensure it is in good working order.
- Change the default BIOS password.
- Ensure the machines have up-to-date antivirus protection

Table 2. The Functional Comparison of ATM Malware Family

Malware Family	Carberp	Qadars	Ploutus	Tyupkin	Anunak	Carbanak
Group	Carberp, Pawn Storm or APT28				Anunak hacker group	Carbanak criminal gang
Identified by the Internet security companies	Federal Office for Information Security, BSI (Germany) and Trend Micro (Taiwan).	Symantec, Microsoft (US) and Sophos.	Symantec, Microsoft (US)	Kaspersky (Russian/UK)	Group-IB (Russia) and Fox-IT (The Netherlands)	Kaspersky (Russian/UK)
Malware Successor (initially based on)	Zeus, Rovnix, RDPdor, Hodprot, and Origami	Zeus, Zbot				Carberp (source code) + Anunak (Wincor ATMs)
Finding Time	2009	May 2013	August 2013	March 2014	December 2014	2015
Victim Location	Russian	Netherlands, France, Canada, India, Australia, and Italy	Mexico	Eastern Europe, the U.S., India, China, Russia, Israel, France and Malaysia.	Eastern Europe, the U.S.	Russia, the United States, Germany, China and Ukraine

Table 3: The Behavioral Attribute Comparison of ATM Malware Family

Category	Case	1	2	3
Who	An organized criminal group name	Carberp, Pawn Storm or APT28	Unlimited Operations	Russian Mafia
	Suspect numbers	8	8	19
	Arrest by	Russia	USA	Taiwan
	Arrested suspects name (from Newspaper)	Germes and Arashi (Alias)	Elvis Rafael Rodriguez, Emir Yasser Yeje, and Alberto Yusi Lajud-Peña	Andrejs Peregudovs, Mihail Colibaba and Nikolay Penkov
What	USD theft in an ATM looting	\$1 Billion	\$45 Million	\$2.6 Million (NT\$83.27 Million)
When	From plan to ATM heist	2009 ~ February 2015	December 2012 and February 2013	July 2016
	Arrest date	March 2012	May 2013	July 2016
Where	ATM location	Moscow in Russia	New York in USA (More than 24 countries)	Taipei City, New Taipei City, and Taichung in Taiwan
How	Money from	the financial institution itself	Prepaid Debit Accounts	the financial institution itself

V. PROPOSED STRATEGY ON ICT GOVERNANCE

Cybercrime prevention requires the participation of Internet users or enterprises to maintain personal or commercial data, and achieve a comprehensive understanding of cybercrime

perpetrators. The whole society should be encouraged to participate more fully and effectively in cybercrime prevention in order to provide for a harmonious online world [16]. A supplementary strategy is intended to achieve the goal of information security. This method can assist banks or law

enforcement agencies in dealing with today's ever-increasing ATM heist. The proposed ICT governance framework in online ATM heist management is discussed into four categories (Figure 1): capable people, efficient process, effective technology, and data governance.

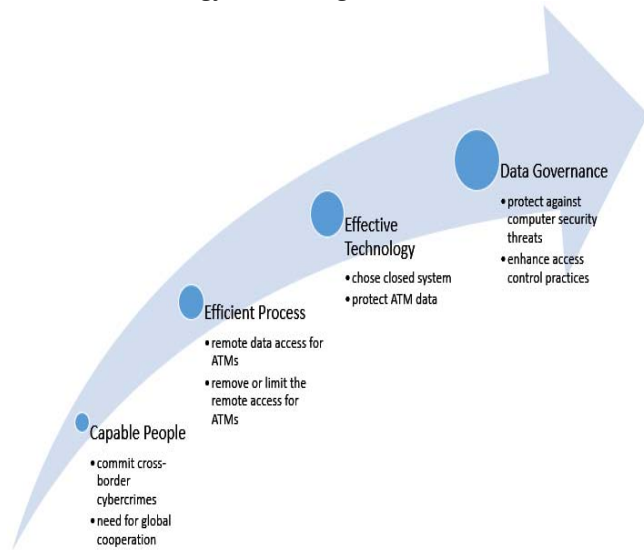


Figure1: ICT Governance Framework in Online ATM Heist Management

A. Capable People

1) Commit Cross-Border Cybercrimes

More and more organizational crime groups use the transnational characteristics of the Internet to evade legal sanction. Cybercrime groups try their best to make geography irrelevant, commit their crimes in cross-border cybercrimes, including online fraud, online gambling, cyber pornography, and hacker attacks. Banks in many countries are becoming new targets of several independent Russian cybercrime groups. Once the attackers successfully compromise the bank's network, the targets are money processing services, ATMs and financial accounts [8]. These cybercriminals use multiple stealing techniques and respond to new security measures with zero-day attack methods to bypass them. They also use stolen money to stay out of jail [12].

2) Need for Global Cooperation

Seeking mutual legal assistance of international cooperation and assistance is a complex, time-consuming process. Arresting some groups or disabling their botnets is not enough to stop them. In March 2012, the 8-member arrest of Department K group in Moscow by the Russia Ministry of Internal Affairs (Министерство внутренних дел) is a great example of international collaboration between both private industry research and international law enforcement (see the case 1 in Table 3)[1, 4, 18]. The only way of fighting them is by the global cooperation of public-private partnership.

B. Efficient Process

The hacking of bank's ATM exposes its careless management to cyber-attacks, highlights the awareness of

information malicious activities, and takes preventive measures.

1) Remote Data Access for ATMs

ATMs need a remote access to communicate with bank data, so network attacks are also a possibility. Some ATMs have wireless modems or Wi-Fi enabled and communication over the public Internet. Others have dedicated connections [9]. There is a trade-off between convenience and security. If convenience increases, security must decrease. The idea of a trade-off just implies a decision to be made with full comprehension of both the upside and downside of a particular choice.

2) Remove or limit the remote access for ATMs

Availability of access to bank ATMs from internal network segments opens great opportunities for the hackers [5]. Security holes or mistakes of system configuration in the internal bank network left sensitive databases exposed to hackers. The strategy should remove or limit the remote access for ATMs.

C. Effective Technology

1) Chose Closed System

Crimeware-as-a-service involves selling exploits and tools for computer trespass. Once attack tools are in place, buyers can rent them to deliver a variety of attacks. Active crime groups have recognized the benefits of the Internet [16]. A bank system should have the boundary of closed system for safety concerns [6]. A closed system has no external interactions and is an isolated system which exchanges neither matter, nor information with its environment. No interactions can take the form of information or material transfers into or out of the system boundary. Internet is not created for security concerns. Once the computers or ATMs are connected to the Internet, no one can guarantee its security.

2) Protect ATM Data

Internal IP Address, computer name and device name should be difficult to match them in an internal network. As far as ICT governance is concerned, this kind of data is limited to key persons or computers. The security of information systems should be reassessed periodically, as the requirements of cyber security vary over time. This raises serious concerns on ATM protection.

D. Data Governance

1) Protect against Computer Security Threats

There are a number of measures that can be adopted by banks to detect, prevent, and minimize the cybercrime damage on the Internet. Banks may implement a number of organizational policies to protect against computer security threats. Moreover, banks need to provide information security training to staffs, increase their awareness of the Internet dangers, and create effective practices to prevent its happening [16].

2) Enhance Access Control Practices

The ATM operation is continuing to become more complex, difficult, and costly. When Microsoft has ended support for Windows XP, most ATM manufacturers still continued to use Windows XP [8]. The access controls of ATM theft still leave

much to be desired. Security risks arise and need to be managed. They are networked devices that have many potential weaknesses if not carefully configured, updated and physically secured. It is important to improve the security controls within banks. Although security controls can never be perfect to implement and expensive to deploy, it remains of critical importance for security measures to be continually managed, reviewed and improved. Insufficient budget can never be used as the reason for not taking action [16]. The default setting for any users is no or limited access. If nothing has been specifically configured for an individual or the groups, users should not be able to access that resource. Banks should enforce strict access criteria, and pay more attention on limiting and monitoring the usage of administrator and other powerful accounts.

VI. CONCLUSIONS

ICT innovations are not only set to bring enormous benefits to the general public, but also bring new technological risks to individuals and businesses. Cybercrimes have rapidly evolved for the dissemination of malware. Criminals increasingly use sophisticated tools and methods to commit their cybercrimes. Most ATMs are still running Windows XP, which is first released in October 2001. The malware is being continuously updated. Old 15-year-old system often opens security holes for hackers. There will be a persistent increase of ATM robbery around the world. The ATM withdrawals happened so quickly that none of the financial banks involved noticed in time to stop the perpetrators. ATM technologies are evolving fast and making payments more convenient. It is our sincere hope to bring the technical details to the attention of information security specialists, and to minimize risks by preventing information security incidents. A small sacrifice in convenience can be useful to prevent an attack in the ATM's door. The ICT governance should be employed by banks to heist ATM money with more barriers.

ACKNOWLEDGMENT

This research was partially supported by the Ministry of Science and Technology of the Republic of China under the Grants MOST 107-2221-E-015-002-.

REFERENCES

- [1] Bitdefender, "Carberp Team Arrested in Russia after Three-Year Run," <http://www.bitdefender.com/security/carberp-team-arrested-in-russia-after-three-year-run.html>, 2013.
- [2] Broadhurst, R., Grabosky, P., and Alazab, M., "Organizations and Cyber crime: An Analysis of the Nature of Groups engaged in Cyber Crime," *International Journal of Cyber Criminology (IJCC)*, vol. 8, no.1, pp. 1–20, 2014.
- [3] Driehuis, E. and Bij, J., "Anunak (aka Carbanak) Update," <https://www.fox-it.com/en/press-releases/anunak-aka-carbanak-update/>, 2015.
- [4] Ferguson, P., "Russian CARBERP Arrests Renew Optimism on International Cybercrime Prosecutions," <http://blog.trendmicro.com/trendlabs-security-intelligence/russian-carberp-arrests-renew-optimism-on-international-cybercrime-prosecutions/>, 2012.

- [5] Group-IB and Fox-IT Research, "Anunak: APT against Financial Institutions," https://www.fox-it.com/en/files/2014/12/Anunak_APT-against-financial-institutions2.pdf, 2014.
- [6] Impagliazzo, J. and McGettrick, A., *Information Systems: What Every Business Student Needs to Know*, NW: Taylor & Francis Group, 2016.
- [7] Jeffries, A., "Cyber Caper: behind the Scenes of the \$45 Million Global ATM heist," <http://www.theverge.com/2013/5/13/4326336/cyber-caper-behind-the-scenes-of-the-45-million-atm-heist>, 2013.
- [8] Kaspersky Lab, "Carbanak APT: The Great Bank Robbery," https://securelist.com/files/2015/02/Carbanak_APT_eng.pdf, 2015.
- [9] Kessem, L., "Carbanak: How Would You Have Stopped a \$1 Billion APT Attack?," <https://securityintelligence.com/carbanak-how-would-you-have-stopped-a-1-billion-apt-attack/>, 2015.
- [10] Kumar, M., "Tyupkin Malware Hacking ATM Machines Worldwide," <http://thehackernews.com/2014/10/hacking-ATM-machine-tyupkin-malware.html>, 2014.
- [11] Maor, T., "Carberp Source Code for Sale — Free Bootkit Included," <https://securityintelligence.com/carberp-source-code-sale-free-bootkit-included/>, 2013.
- [12] Matrosov, A., "All Carberp Botnet Organizers Arrested," <http://www.welivesecurity.com/2012/07/02/all-carberp-botnet-organizers-arrested/>, 2012.
- [13] Microsoft Malware Protection Center, "The Exploit Malware Family," <https://www.microsoft.com/security/portal/mmpc/threat/exploits.aspx>, 2016.
- [14] Osborne, C., "Suspected Hackers behind Carberp Botnet, Eurograbber Arrested," <http://www.zdnet.com/article/suspected-hackers-behind-carberp-botnet-eurograbber-arrested/>, 2013.
- [15] Pan, J., "Key ATM Heist Suspects Turned Over to Prosecutors," <http://www.taipeitimes.com/News/front/archives/2016/07/19/2003651333>, 2016.
- [16] Smith, R. G., Cheung, R. C. C., and Lau, L. Y.C., *Cybercrime Risks and Responses Eastern and Western Perspectives*, England: Hampshire, Macmillan Publishers Limited, pp. 67-211, 2015.
- [17] Wallace, G., "Hackers Stole from 100 Banks and Rigged ATMs to Spew Cash," <http://money.cnn.com/2015/02/15/technology/security/kaspersky-bank-hacking>, 2015.
- [18] Warner, G., "CyberCrime & Doing Time: A Blog about Cyber Crime and related Justice Issues. Russian MVD announces arrest of CARBERP gang," <http://garwarner.blogspot.tw/2012/03/russian-mvd-announces-arrest-of-carberp.html>, 2012.



Dayu Kao is an Associate Professor at Department of Information Management, College of Police Science and Technology, Central Police University, Taiwan. He is responsible for various recruitment efforts and training programs for Taiwan civil servants, police officers or ICT technicians. He has an extensive background in law enforcement and a strong interest in information security, ICT governance, technology-based investigation, cyber forensics, human resource development, and public sector globalization. He was a detective and forensic police officer at Taiwan's Criminal Investigation Bureau (under the National Police Administration). With a Master degree in Information Management and a PhD degree in Crime Prevention and Correction, he had led several investigations in cooperation with police agencies from other countries for the past 20 years. He can be reached at camel@mail.cpu.edu.tw.