International Journal of Cyber Criminology
Vol 12 Issue 1 January – June 2018

Routine Activities in a Virtual Space: A Taiwanese Case of an ATM Hacking Spree

Ming-Li Hsieh[1]
University of Wisconsin-Eau Claire, United States of America

Shun-Yung Kevin Wang[2]
University of South Florida St. Petersburg, United States of America

Abstract

Routine activity theory (RAT) was initially proposed to explain shifts in urban crime rates in the late 1970s, and has subsequently been applied to predictions of predatory criminal or victimization events. Despite a number of studies attempting to apply RAT to the vast array of crimes now taking place in a virtual environment such as phishing, fraud, malware infection, identify theft, computer viruses and cyber stalking on the Internet in Western countries, little is known about whether RAT could address automatic teller machine (ATM) hacking in an Asian setting. The current study applies RAT in order to examine a high-profile case of European hackers programming ATMs in Taipei to "spit out" cash netting the thieves $2.6 million dollars. The results indicate that the Taiwanese case is well covered by the doctrine of RAT. Moreover, this study bolstered the neo-ideology of "cannikin law" within cyber crime, in which the effectiveness of cyber security and levels of risk would depend on the magnitude of guardianship (in reference to the idea that any protection measure is only being as strong as its weakest link).

Keywords: Routine Activity Theory, White Collar Crime, Cyber Crime, Cyber Security.

Introduction

Since the first web browser appeared online in the early 1990s, the growth of the Internet and related modern information technology has escalated dramatically. Human activities today transmit valuable information in cyberspace where the Internet is a fast, open, omnipresent ecosystem with content-rich service and without geographical boundaries (International Telecommunication Union [ITU], 2016). Accompanied with widely available Wi-Fi and telecommunication systems allowing users to access the Internet through a wide variety of devices, a seemingly limitless amount of digital information can now be easily and quickly transferred from one end of the world to the

[1] Assistant Professor of Criminal Justice, University of Wisconsin-Eau Claire, P.O. Box 4004, Hibbard 428, Eau Claire, WI 54702, USA. Email: hsiehm@uwec.edu
[2] Associate Professor of Criminology, University of South Florida St. Petersburg, 140 Seventh Avenue South, St. Petersburg, Florida 33701, USA. Email: ShunYungWang@mail.usf.edu

other (Britz, 2013). Despite its origins within the Department of Defense's DARPA project for the purpose of securing communications within the military, the Internet has become an essential part of ordinary people's daily lives across international borders. For example, on average, 89 percent of people in the United States use the Internet every day, followed by Europe (80), the Middle East (72), Latin America (64) and Asian/Pacific countries (58) (PEW, 2017). The Internet, a "network of networks" (Castells, 2002), has expanded individual and group users' physical surroundings to include virtual activities, including communications, information distribution, entertainment, education, and business investment and transactions.

Arguably, cyberspace is not inherently evil but opportunities afforded by a virtual environment may fuel the illegitimate network life of cyber crime. When valuable financial and banking transactions are linked with tremendous business profits from the web, each segment of the transaction can become a target of criminals' rational choice. These systems have few deterrent factors or social control mechanisms, and as a result, motivated offenders are provided with a number of alternatives for committing cyber crimes that may not necessarily require sophisticated skills, opportunities and means (Jaishankar, 2008). The convenience of the Internet is like a magnet that attracts more personal devices, critical infrastructure (e.g., energy, transportation), and even life-saving equipment (e.g., pacemakers) to interact on the information "superhighway", and the Internet of Things (IoT) is one of the converging trends reflecting the growth of inter-connected networks (Singer & Friedman, 2013). Potential victims, lacking adequate protection, converge with offenders in cyberspace and expose themselves to high levels of security risk. Further, cyberspace provides complete dissociative anonymity and invisibility relative to the traditional physical space for motivated offenders (Jaishankar, 2008). These elements can all be attributed to the significant rise of cyber crime.

Cyber attacks have now become the second-most reported economic crime; one that affects 32 percent of organizations and is responsible for losses averaging over one million dollars per incident (PWC, 2016). Globally, cyber crime cost the world $3 trillion in 2015. There is no doubt that the cost will continue to increase and is projected to climb to 6 trillion annually by 2021 (Cybersecurity Ventures, 2017). At the individual level, from 2012 to 2016, there have been 1.4 million cases of cyber crime reported to the FBI, and a total reported loss of $4.63 billion across types of cyber victimization such as data breaches, phishing, identity theft, harassment, fraud, varied malware, extortion, and advanced fee frauds (FBI, 2017).[3]

Given that various forms of cyber crime have been acknowledged as some of the biggest threats to individuals and businesses (Cybersecurity Ventures, 2017), criminologists have attempted to understand the nature of cyber crime, the characteristics of cyber criminals, and to enhance cyber crime control and prevention. Although proposed decades ago, routine activity theory (RAT) by Cohen and Felson (1979) has not only been proffered as an explanation for contemporary cyber crime and "virtual criminality" primarily in Western countries (Grabosky, 2001; Leukfeldt & Yar, 2016), but also has

[3] The FBI is traditionally not a good source of data about cyber crime, as their numbers generally under estimate the seriousness of cyber crimes. IC3 collects "complaint" data, but many harmful crimes like identity theft, for example, are reported to the FTC where victims would be advised to also report to local police, credit bureaus, and bank/financial institutions.

been widely applied to cyber victimizations such as fraud (Pratt, Holtfreter, & Reisig, 2010; van Wilsem, 2013), phishing (Hutchings & Hayes, 2009; Leukfeldt, 2014; Paek & Nalla, 2015), identify theft (Reyns, 2013), malware infection (Holt & Bossler, 2009, 2013), and stalking (Reyns, Henson, & Fisher, 2011).

Currently, little is known about whether RAT could address a new form of logical attacks[4] against automatic teller machines (ATM) (so-called ATM hacking) in Asian settings. Before generating new theories with a specific focus on the "novelty" of cyber crime, as Yar (2005) noted, researchers need to assess to what extent that RAT can be applied to crimes in virtual space by expanding its explanatory power to studies of varied types of cyber crime and victimization. Therefore, the current study seeks to fill the literature gap in RAT by examining a recent high-profile cyber crime case involving European hackers who targeted ATMs in Taiwan. This case study contributes to the field by highlighting legal documents, case reports and interviews with the primary cyber crime investigator and forensic analysts in Taiwan. The paper begins with an articulation of the criminological framework, followed by the details of a recent criminal case of ATMs that were targeted by a group of organized criminals via the Internet. Finally, policy implications about cyber security improvement and crime prevention are discussed.

Cyber crime Victimization and Routine Activity Theory

Since the publication of Cohen and Felson's (1979) routine activity theory, which was initially proposed to understand patterns and upward trends of predatory criminal events in the historical context of changing economy, the theory has been applied to a wide spectrum of victimization experiences such as victimization in the workplace (Wooldredge, Cullen, & Latessa, 1992), theft (Argun, & Dağlar, 2016), larceny (Mustaine, & Tewksbury, 1998), burglary (Argun, & Dağlar, 2016; Breetzke & Cohn, 2013; Louderback & Roy, 2018), fraud (Holtfreter, Reisig, & Pratt, 2008), robbery (Groff, 2007; Louderback & Roy, 2018; Spano, & Nagy, 2005), vandalism (Tewksbury, & Mustaine, 2000), and aggravated assault (Louderback & Roy, 2018). Researchers in cyber criminology have argued that the conventional elements of RAT could be adopted to explain cyber victimization facilitated or commissioned by varied means of information technology (Grabosky, 2001; Leukfeldt & Yar, 2016).

Briefly, for a crime to occur, RAT purports that three essential elements must be present: likely offenders, suitable targets, and the absence of capable guardians (Cohen & Felson, 1979). The theory is not primarily interested in understanding an offender's motivation but rather focuses on the characteristics of crime where "the spatio-temporal organization of social activities helps people to translate their criminal inclinations into action" (Cohen & Felson, 1979, p. 589). Offenses become a viable alternative in social situations structured by the legitimate daily routines in which property and/or people appear to be attractive targets for those who are motivated. It is an interdependent relationship between the predispositions for committing offenses, target suitability derived from routine legitimate activities and the degree of inadequate protection and supervision provided by guardians at all levels. Lacking one of these elements the crime is less likely to take place, however, Cohen and Felson (1979) further indicated that increasing the opportunity of enjoying rewards and benefits obtained from illegal activities could also

[4]A series of sophisticated actions that may involve using malicious software, hardware, or a combination of both, to commit crimes against ATMs.

enhance the propensity for predatory violations. Given the substantial rise in economic cyber crime and new varieties of cyber victimization as well as the grand scale of financial losses (Levi, 2017), criminologists have attempted to understand the ecological niche of cyber crime, specifically those aspects of cyber accessibility associated with subjects, approaches, time and location in a virtual space.

Motivated Offenders

Although it has been argued that RAT might not directly apply to the structure of cyberspace as it often appears disorganized temporally and spatiality in the virtual environment (see Yar, 2005), for a cyber crime to take place studies have found that the basic components of RAT must be present (Taylor, Caeti, Loper, Fritsch, & Liederbach, 2006; Bossler & Holt, 2009; Holt & Bossler, 2009, 2013; Hutchings & Hayes, 2009). Still, almost everyone would agree that there are "motivated offenders" out there seeking appropriate opportunities to commit offenses which is a required element in understanding all types of crime (Cohen & Felson, 1979) including cyber crime (Taylor et al., 2006; Bossler & Holt, 2009; Holt & Bossler, 2009, 2013; Hutchings & Hayes, 2009).

Although the very nature of cyberspace allows perpetrators not to be physically close to potential victims in order to compromise victims' computers and, more importantly, the information/data stored on them (Taylor et al., 2006; Eck & Clarke, 2003), there are spatial properties in the virtual world that can be identified as partially congruent with physical space (Yar, 2005). To initiate a hack and calculate the spatio-temporal "timing, tempo and rhythm" (see Hawley, 1950) of launching an attack, for instance, offenders might linger in cyberspace waiting for any infected tools to be "clicked" by online users in order to invade a user's device. Malware is a typical way to open the "backdoor" of an information system for hackers in a cyber attack, after the inception of social engineering (Mitnick, 2001). To best increase the exposure of prospective victims, "offenders will attempt to keep their files active and circulating for as long as possible" in any cyber location (e.g. email attachments, social media sites, web pages, online advertisement, chat rooms, portals) and "victims [would] play an active role" in initiating hidden malware (Holt & Bossler, 2013, p. 423). In this sense, the likelihood of victimization depends on the degree to which a victim's online behavior is virtually proximate to a perpetrator's programmed malware, such as computer viruses, worms, Trojan horses, ransomware, spyware, and other malicious codes (Bossler & Holt, 2009; Holt & Bossler, 2013). Similarly, to deceive potential victims, bogus websites with embedded malware that have to constantly change online addresses (before being detected and shut down) often are facilitated by messages with hyperlinks to shorten the virtual distance.

Hutchings and Hayes (2009) indicated that online banking and computer use are risk factors for phishing victimization. Internet users who engage in the most online banking are more likely to be attacked by motivated offenders even though their computers and other devices have been protected by some level of a firewall. Users who engage in computer deviance such as using pirated software and media, visiting pornographic sites and viewing obscene materials many of which mimic "hacker-like" behaviors (see Rogers, 2001) would increase the chance of being targeted while online (Holt & Bossler, 2009). Another study revealed that users who access high speed Internet in order to take advantage of prompt sharing and connectivity in disseminating information are more likely

to be victimized in some way by cyber perpetrators (Hinduja, 2001). As these examples illustrate with just a few "clicks" on the Internet, prospective victims can be redirected to virtual locations that place users in much closer proximity to cyber criminals (Yar, 2005). In other words, users' online activities with their IP addresses might signal their "cyber locations" and show in-use devices or systems that are potentially vulnerable to online perpetrators.

Suitable Targets

A suitable target can be "a person, an object or a place", and an assessment of that subject depends on cumulatively weighted factors (e.g. visibility, value, accessibility) which might attract offenders to commit an offense (Argun, & Dağlar, 2016, p. 1189).Although offenders would interpret suitable targets differently, in general for offenders, a suitable target would increase the likelihood of "gain" (e.g. benefits, profit, value, ego satisfaction and achievement) and the possible rewards of illegal activities would outweigh the potential punishment and consequences (Argun, & Dağlar, 2016; Bossler & Holt, 2009).

Yar (2005, p. 419) indicated that "valuation of targets" is a crucial factor for cyber crime. Criminals can commit a wide array of different cyber crimes, ranging from compromising and damaging computer systems, stealing personal and organizational data and intellectual property, stalking and harassing Internet users, to intervening in online services for trading, selling, and exchanging services, but these targets in cyberspace are informational in nature. To criminals, high value and portability are desirable target characteristics, and those found in cyberspace are nearly "weightless". Selecting suitable individuals or organizations in cyberspace with higher levels of vulnerability is necessary for obtaining a greater likelihood of "hit rates" with respect to lucrative rewards, financial gains or other malicious purposes.

In terms of victimization, Internet users with certain characteristics or habits have created opportunities for perpetrators to reach them. A large pool of suitable targets are older, with inadequate account and payment settings (Holtfrete & Mears, 2015), low self-control and a tendency to engage in remote shopping (Reisig & Holtfreter, 2013). Reyns (2013) examined risk factors for identity theft victimization and determined that those who are male, older, have a higher income and exhibit routine online behaviors, such as using instant messaging, e-mail, downloading (e.g. podcasts, music, films), buying products or services online, and managing finances online through online banking systems, are more likely to be victimized. For consumer fraud victimization, Internet users' socioeconomic backgrounds would affect their online activities, and those who spend more time surfing the net (Pratt et al., 2010), consuming online (Pratt et al., 2010; van Wilsem, 2013) and visiting online forums (e.g. Facebook or other social media sites) (van Wilsem, 2013) are at greater risk of being targeted by fraudsters.

In another example of target suitability, a prospective victim's online personal information such as social media or instant messenger IDs, or e-mail can be sufficient for perpetrators to pursue attacks, however, some relatively private personal information (e.g. photos, videos, sexual orientation, gender, relationship status) could also be valuable to offenders and might make targets more desirable than other targets without the traits listed above (Reyns et al., 2011). Marcum, Higgins and Ricketts (2010) revealed that high school students who spend more time in chat rooms and provide more personal or in depth information (e.g. demographic background, school, family status, pictures,

emotions, activities, sexual preferences) online are at higher risk of receiving sexual solicitations. This study also indicated that college students who have received unwanted sexually explicit materials were more likely to have posted personal profile and daily life information on social networking and were communicating with people via their electronic devices and the Internet. All of these online activities appear to be related to making oneself a more attractive target to offenders.

Absence of Capable Guardians

Cohen and Felson (1979: 605) argued that a lack of effective social control and punishment mechanisms would result in an increase "in the certainty, celerity and value of rewards to be gained from illegal predatory acts" which may result in more predatory crime taking place. In a similar vein, without capable guardianship in cyberspace, whether it is at the governmental level, organizational level or individual level, there is an increase of likelihood for illegal gains and the propensity for victimization (Bossler & Holt, 2009; Marcum, Higgins, & Ricketts, 2010; Reyns et al., 2011; Williams, 2016). Cyber guardianship ranges widely from informal guardians (e.g. in-house network administrators, ethical private and public computer users) to formal guardians (e.g. firewalls, anti-virus software, IT staff, severity monitors and supervisors). Furthermore, whether the guardian is willing to supervise and intervene when necessary, as well as able to detect potential offenders, is practically important (Reynald, 2010). All of these efforts are critical for deterring potential criminals and controlling and preventing the convergence of motivated offenders and suitable targets in cyberspace (Yar, 2005).

Despite the argument that there is no significant effectiveness in the use of email filters (Hutchings & Hayes, 2009) and physical computer guardianship (Holt & Bossler, 2009), Williams (2016) found that those online users who were less likely to adopt passive physical guardianship measures such as using an email filtering system, installing anti-virus browsing and using only one computer were 1.32 times more likely to be victimized. Moreover, those less likely to be victims of identity theft were those more likely to use avoidance personal guardianship, for instance, spending less time online and doing less shopping and banking online. Another study showed that temporal guardians such as having a friend visible in a place where the Internet is being used and using it in places (e.g. living room, school computer lab) where there is some level of guardianship reduces the likelihood of receiving online sexually explicit material and receiving online harassment, respectively (Marcum et al., 2010).

In addition, routine high risk online behavior may also include using unguarded networks through connecting to any public Wi-Fi (e.g. airport, subways, coffee shops, bus, restaurants, hotels). In other words, individuals often put themselves at greater risk of being hacked without realizing it. As Reyns (2013) explains typing sensitive information (e.g. social security number, account numbers, passwords, banking information, credit cards) while connected to a Wi-Fi network without adequate cyber security protection allows motivated perpetrators who are in the same time and space (on the same network) to find opportunities to penetrate computers and access personal data.

In summary, a number of studies have adopted RAT to explain cyber crime across types of victimization and support the concept of the convergence in time and space of motivated offenders, suitable targets and the absence of capable guardians that leads to crimes occurring in cyberspace (Choi, 2008; Holt & Bossler, 2009, 2013; Hutchings &

Hayes, 2009; Leukfeldt, 2014; Marcum et al., 2010; Ngo & Paternoster, 2011; Paek & Nalla, 2015; Pratt et al., 2010; Reyns, 2013, 2015; Reyns et al., 2011; van Wilsem, 2013). Despite a consensus of support for this approach, arguments of applicability may remain (see Leukfeld & Yar, 2016; Yar, 2005) as little is known about whether the RAT could be applied to ATM hacking and whether the three RAT elements could be used in an Asian setting. Therefore, the current study examines a recent Taiwanese high-profile cyber crime case and extends the utility of RAT to Taiwanese cyber crime.

A Case of Cyber Crime

The current study focuses on a First Commercial Bank (FCB) ATM heist case in Taiwan using RAT elements. This study contributes to the field of cyber crime by examining legal documents, investigations and analysis reports. Moreover, the current study interviews a computer crime forensic analyst who is a senior special agent in the Ministry of Justice Investigation Bureau (MJIB).[5]

Analytic Plan

Besides examining both public and unpublished case documents[6], researchers obtained the approval of IRB, and contacted the MJIB agents for interviews concerning the FCB case. After receiving an explanation of the research purposes and reviewing the interview questions, the primary investigator (S)[7] signed the informed consent form and agreed to share his insights and perspectives on cyber crime.

Case Profile: FCB ATMs Hacking in Taiwan

On 11 July, 2016, international cyber criminals targeting ATMs in Taiwan shocked authorities with a quick and sophisticated strike. The cyber attack involved an Eastern European organized crime group consisting of 22 suspects (code-named "Cobalt")[8] from 8 countries and targeted one particular type of ATM (PC 1500XE) manufactured by Wincor Nixdorf International which was adopted by financial businesses globally (Taipei District Prosecutors Office [TDPO], 2016). The unknown attackers hacked 41 ATMs at 22 branches of the FCB, programmed the system to dispense cash as "jack potted" slot machines, and arranged mules to collect a total of NT $83.27 million dollars in cash (approximately US $2.63 million dollars). On 17 July, 2016, three mules were apprehended by the police in Taiwan and TDPO issued an arrest warrant for the remaining 19 suspects who had fled. Later in September, the TDPO charged the mules with multiple criminal offenses against computer security and recommended a 12-year-sentence for each offender.[9]

[5]MJIB in Taiwan is equivalent to the FBI in the United States.

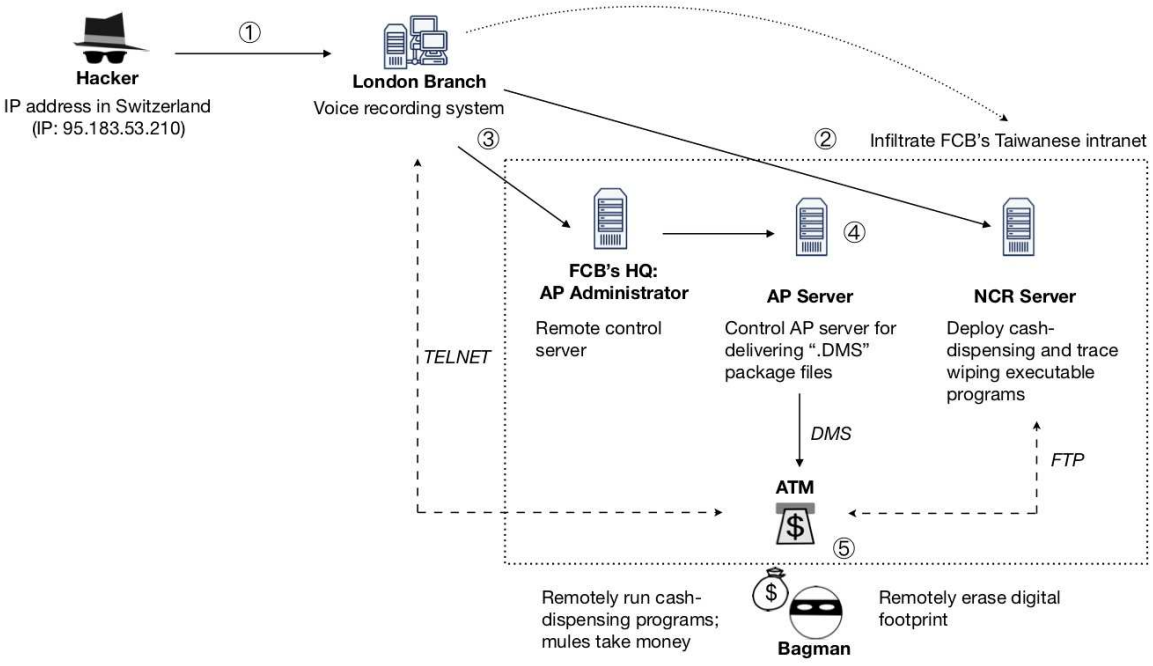
[6]Although Tai-Wei Chou, cyber crime section chief at MJIB did not receive our interview, detailed study notes of the crime's reconstruction and the modus operandi are provided.

[7] Given confidentiality concerns, this study used "S" to refer to the investigator's statements throughout the manuscript.

[8] Hackers used a publicly available security program (i.e. Cobalt Strike) to penetrate the bank's networks (Sancho, Huq & Michenzi, 2017).

[9] Taiwan has adopted collegial panels for use in the legal system. A collegial panel is composed of three to five judges depending on the level of the court.

Figure 1. Network of FCB ATM Jackpotting



The modus operandi utilized by the Cobalt group to penetrate the FCB network, according to Tai-Wei Chou, cyber crime section chief at MJIB, can be broken down into five significant steps (see Figure 1). First, digital forensics show that this incident began with an IP address in Switzerland on May 31, 2016. Hackers penetrated FCB's branch in London, accessed the banks' voice recording system, and successfully stole an administrator's credentials in order to infiltrate the FCB's Intranet. Second, after compromising the voice recording system, hackers dispatched five executable files related to cash-dispensing (cnginfo.exe, cngdisp.ex, and cngdisp_new.exea) and trace-wiping (cleanup.bat and sdelete.exe) on the NCR server. Third, by using credentials obtained from the London branch, a hacker also remotely breached the administrator's account and compromised employees' computers in Taiwan's FCB's headquarters. This deeper penetration gave the hackers remote control over application server (AP) frameworks. Fourth, when the AP servers were taken over, hackers could upload and deliver fake package files (with the filename extension ".DMS") that are only recognized by ATMs for updating programs. After the ATMs finished updating with the disguised software, the ATMs would turn on a telnet service that enables a connection between remote computers and computers within the ATMs and also builds a file transfer protocol (FTP) connection which allowed ATMs to download pre-installed executable files from the NCR server. Hackers completed deployment on July 4, 2016 and arranged mules to approach designated ATMs from July 9 to July 11, 2016. At the day of the attack, the mules contacted hackers who remotely controlled the ATMs via telnet service and

downloaded and executed the programs for cash dispensing and digital footprint removal through an FTP connection.

Notably, the FCB incident was well orchestrated and coordinated, and offenders played specific roles to complete an array of different tasks. In addition to the hackers, 14 bagmen were responsible for multiple detailed tasks such as standing sentry, withdrawing cash from ATMs, bagging the cash, transporting money, transferring and hiding the cash. To avoid detection by law enforcement, criminals changed lodgings, used burner phones with disposable numbers and SIM cards, and rotated the stolen cash around different hotel rooms, car trunks, luggage, and even in public lockers at the Taipei mass rapid transit (MRT) station.

Cover ups are not uncommon in cyber incidents, especially for financial institutions and corporations because of their concerns for their business reputation in the industry, working relations with the administration, and potential psychological impacts on customers. In this case, however, FCB decided to work with the authorities. Because of the mass media coverage after the ATMs were looted, citizens were able to identify suspects and report their suspicious behaviors standing in front of ATMs with backpacks, in turn, leading to the arrest of three bagmen.

Discussion

This high profile Taiwanese case raised considerable national and international attention for several reasons. First, even though Taiwan is one of dozens of ATM jackpotting cases committed by similar methods and allegedly the same Eastern European gang (e.g. Estonia, Malaysia, Thailand, Britain, Russia, Spain, Poland) (Finkle, & Wu, 2017), Taiwan is the first state to arrest, prosecute and convict three members of the Cobalt group (Liberty Times, 2016). Second, the case was closed not only by sentencing the criminals for an average 4.8 year term of imprisonment but also, authorities recovered more than 90 percent of the stolen money (approximately is 2.4 million US dollars) within a few days. Third, this case highlights the Taiwanese authority's effectiveness in cyber crime investigation and computer forensics. The FCB incident also initiated the realization that cyber criminals could be brought to justice if authorities could dominate the intelligence race. For this to occur, cyber crime investigators must have the tools to detect hidden and potential cyber attacks that develop through rapidly innovated hacking techniques. Success also involves the ability to obtain good evidence, and effectively employ courtroom workgroups (see Eisenstein, & Jacob, 1977) that clearly understand cyber crime.

Additionally, this case provided insightful information about how criminals utilize cyber attack techniques to rob banks in the era of the Internet. The experience of Taiwan's FCB in this case can be considered a useful lesson that may be able to guide American authorities as they investigate the most recent American ATM jackpotting case that happened in early 2018 and lost over 1 million dollars (see Volz, 2018). Even though the case is currently under investigation, we speculate the modus operandi used in the United States would be similar to the FCB case or other international ATM jackpotting cases. More importantly, the FCB case can be used to expand a routine activities theoretical framework of ATM hacking where the convergence in physical space, cyberspace, and time offers an enticing opportunity to commit cyber crime.

1. The Presence of Motivated Cyber Offenders

At least fifty percent of Asian Pacific institutions reported increasing economic crime as well as heightened concern about the pervasive and sustained threats of cyber attacks (PWC, 2014). With the techniques and tools adopted by hackers becoming more sophisticated, Asian countries such as China, Taiwan, and South Korea with emerging lucrative markets and increasing use of the Internet are at greater risk of cyber attacks (Antonescu & Birăub, 2015). Financial service institutions in these countries, for example the FCB in Taiwan, may have a relatively lower level of cyber security in general compared to more economically complex countries. As Antonescu and Birăub (2015) explain, Internet users may still underestimate the vulnerability of "transmission channels" (e.g. e-mails, chat rooms, discussion forums, social media, messenger, instant messaging or other online services) that could be utilized for network penetration. As the investigator in this case, "S" theorized:

> …well 'social engineering' is still the primary method that hackers would use to trick you into clicking on something online, maybe an ad, a picture, a posted thread or a link or an attachment enclosed in email. With a 'click away', hackers can gain access to anything regardless of the distance, a smartphone, electronic device, computer, server, system, organization, building, absolutely anywhere within a network. In the FCB case, one alleged explanation for how the hackers got into a voice recording system in the first place is through 'spear phishing' against a specific administrator. This is not about how secure your firewall is. You would eventually be tricked, and hackers know this and could use your action as an extension of attacking.

At this point it already appears that the FCB case is consistent with RAT's first key component — motivated offenders. The clear pattern of advanced persistent attack (APT) (see Singer & Friedman, 2013) against carefully selected targets that are likely to have certain user privileges within the information system makes the motivation of the criminal group more than evident. None the less, this case is also consistent with Yar (2005)'s argument that because of the context of cyberspace, it may be much more difficult to analyze "offenders" under the doctrine of RAT (see Cohen & Felson, 1979). One possibility is that the existence of motivated FCB cyber criminals could be explained by virtual proximity distance. Yar (2005) stated that Internet users are often just a few "clicks" away from many "cyber criminals". As other studies have demonstrated, in cyberspace, perpetrators can compromise a victim's computer and system regardless of physical contacts and geographical boundaries (Taylor et al., 2006; Eck & Clarke, 2003) as long as victims activate hidden malware. In this sense, motivated offenders in cyberspace might not be physically proximate but rather they only need the appropriate attack opportunity which is the same as conventionally motivated offenders in society (Cohen and Felson, 1979). As agent "S" explains:

> Frankly, motivated cyber criminals are everywhere, just like criminals in the physical environment… they are out there but again, the fact is the majority of them almost cannot be identified by us [law enforcement]. Even though Taiwanese authorities did a good job and solved the FCB case, we did not know who was behind this incident; that operated and manipulated the FCB's network. Still, we are closer to identifying and apprehending more members of the Cobalt

> group than any other country. …Compared to criminals in a physical environment, cyber criminals benefit from two distinct features of cyberspace, invisibility and anonymity. This may encourage cyber criminals to commit more crimes or it may entice criminals in a physical environment to switch to committing offenses online.

Despite Taiwanese authorities' success at apprehending three mules from the Cobalt group within six days and the country's High Court sentencing them to fines and incarceration within less than ten months, this swift and certain response may still not generate enough deterrent effect to offset motivated cyber offenders. For example, soon after the FCB incident, Far Eastern International Bank in Taiwan was targeted and hackers attempted to steal 60 million dollars (of which almost all has been recovered) (Reuters, 2017). In a study in Ghana, Danquah and Longe (2011) noted that cyber crimes are invisible, anonymous and involve flexible identities, as well as lack a formal oversight system such as police or vigilantes to patrol or watch over the cyber community. In this sense, the intrinsic nature of cyberspace would reduce the likelihood of being caught by authorities. In other words, criminals who commit offenses in cyberspace might be able to extend the timeframe during which they are able to enjoy the rewards of illegal gains due to inefficient social control mechanisms that are unable to provide the "certainty, celerity and severity of punishment to compete" with emerging new types of crime and victimization on the Internet (Cohen & Felson, 1979, p. 605). This may also be one of reasons that it has been predicted that Taiwan will suffer a substantial number of cyber attacks (Antonescu & Birăub, 2015).

2. Online Target Suitability and Attractiveness

The FCB case is thought to be one of the first times that the international organized crime Cobalt group committed an offense in Taiwan. This means that Taiwanese financial institutions may become more attractive to cyber criminals. First, offenders focused on a specific ATM model manufactured by a Germany company as the suitable target for using their programmed malware that triggered the flow of a large amount of cash from ATMs. Second, cyber criminals exploited the vulnerability of the cyber security defense system and waited for an opportunity to penetrate the system that was created by negligent service provisions. As Investigator "S" relates,

> ...if you are a criminal and you know you are able to infiltrate a large number of ATMs at once, particularly this type of system (PC 1500XE), and you can remotely control ATMs to spit out cash for you in a few seconds, don't you think this is a very attractive and lucrative gain? And I bet you would want to know which country uses this ATM model…

The FCB case also demonstrated that certain aspects of prospective targets would increase the possibility of rewarding a predatory cyber crime. This element, as well as other collectively weighted factors, is all part of a perpetrator's rational analysis of target suitability. Consistent with prior cyber victimization studies, criminals would associate with victims with certain traits (e.g. demographics, accessibility, visibility) (Reyns, 2013; Yar, 2005; Marcum et al., 2010), value (Yar, 2005), or online activities and behaviors (Reyns, 2013; Pratt et al., 2010; van Wilsem, 2013; Marcum et al., 2010; Leukfeldt, 2014)

in order to facilitate a crime. In this way, agent "S" explains, the net of potential victims is widened.

> …as offenders probe deeper into the network to control ATMs, it is possible that the FCB would not be the only victim. Everyone who was tricked by this social engineering should be considered a victim…even if he or she [a victim] did not lose any personal data or files and their computer is still working just fine, for hackers, he or she is still a suitable target. At that point of time, he or she might not be directly linked to financial loss, but might be used to prepare the next move, which eventually would help offenders to gain something.

Phishing, as an instrumental expression of social engineering, is a routine part of the process utilized by a majority of cyber criminals to reach prospective victims (Mitnick, 2001; Soudijin & Zegers, 2012). In a national level study for high cyber crime countries, Kigerl (2012) revealed that overall Europe, Latin America and Asian countries would be more likely to receive phishing attacks than African countries. In general, phishing is less dependent on a victim's demographic and financial characteristics, online accessibility, and visibility. It seems to be successful as long as hackers can reach any one of a large number of signals in a pool that have been sent phishing content via e-mail or other online connections (Leukfeldt, 2014). As reports revealed, Taiwan and other 13 European countries were targeted by the Cobalt group for this type of cyber attack. Therefore, it was hypothesized that when hackers were conducting a worldwide search for suitable access to the specific ATM model they had targeted, the FCB's London branch administrator who had clicked a phishing e-mail provided them the initial opportunity to infiltrate the FCB network (Finkle & Wu, 2017). Future study should explore other factors and explanations in this regard.

3. Examining Guardianship in Cyberspace

It has been argued that financial intuitions in Taiwan face high risk exposure to cyber attacks due to social structural and institutional security imbalances (Antonescu & Birăub, 2015). Although institutional and organizational features provide capable formal guardians (e.g. physical security defense systems, anti-malware software), it is the users' visibility and online activities that are usually linked to security vulnerability (Leukfeldt, 2014). Guardianship like anti-malware physical security systems does not prevent person-based victimizations that often start with social engineering (Holt & Bossler, 2014). These vulnerabilities can easily be exploited by hackers contributing to individual victimization or providing an "infected spot" through which offenders continue to penetrate the system. This is especially true when there are increases in the use of communication and information technology, the extension of all different types of online services and activities supported by using smartphones and other electronic devices with the Internet and through Wi-Fi accessibility. As "S" was able to explain based on investigations he conducted on the basic platforms of potential cyber criminal activities,

> Levels of cyber security depend on the effectiveness of capable guardians provided by organizations working together with users for comprehensive cyber guardianship. Applying 'cannikin law' to cyber security, if the capacity of water in a barrel is determined by the shortest of the wooden staves, then the magnitude of

> cyber guardianship is determined by the weakest security link. Although companies may continue to upgrade their institutional cyber defense system, they can still be undermined by employees or ordinary people whose mistakes result in overall system breaches. People easily make mistakes such as browsing some unprotected websites or opening some phishing messages. These behaviors will reduce the magnitude of cyber guardianship.

Consistent with research by Leukfeldt (2014, p. 554), financial intuitions in Taiwan might not be able to "stop a motivated offender from gaining control over" financial service systems or customers' accounts, yet with certain levels of guardianship, the harm and loss caused by cyber crime could be reduced. In other words, the magnitude of cyber guardianship could be improved by the collective efforts of users and companies.

In the case of FCB, hackers allegedly obtained access credentials from an administrator at the London branch through phishing rather than breaching a physical cyber defense system. From a cyber security perspective, this highlights the problems of personal guardianship (see Leukfeldt & Yar, 2016; Williams, 2016). As in prior studies, personal capable guardianship (i.e. a user's online behavior) is critical in reducing the harm caused by cyber criminals. For instance, users who are aware of the risks of online activities or have some level of technical computer knowledge were less likely to be victims of hacking (Leukfeldt & Yar, 2016). This concept was reinforced by agent "S".

> …I would say, theoretically there are no really 'strong enough' capable guardians in cyberspace to protect users and institutions and to prevent future attacks and realistically, we won't be able to fully stop the potential threat of attacks. In the FCB case for example, I mean if an invisible and anonymous hacker who purposely wants to penetrate a company or steal your information, how would we know that in advance? The odds are really low, right?
>
> Otherwise they wouldn't be called a 'hacker'. In fact, a majority of victims do not know they have been attacked until they have been informed by authorities or companies… a user's online behavior creates vulnerability and could be exploited by motivated offenders…

While it may sound true that if people do not use the Internet for any activities (e.g. shopping, browsing websites, downloading files/music/video, e-mail, messaging), then there would be no cyber crime or cyber victimization, this is an unreal expectation in our society today. For most people, it is nearly impossible not to use the Internet throughout daily life – even traditional line-telephone service switches to Internet technology. Although users and organizations cannot eliminate the risks of being cyber attacked, Williams (2016) states that using both or either physical guardianship and personal guardianship would frustrate cyber criminals and reduce the likelihood of being victimized in cyberspace.

Conclusion

The current study addressed three elements of RAT theory in the context of cyber crime. Support was found for the idea that motivated cyber offenders are out there assessing online target suitability and attractiveness and are most likely to commit offenses when there is insufficient capable guardianship in cyberspace. Using the recent case of a

FCB ATM heist in Taiwan, we were able to examine a type of victimization that is different from previous studies (Argun, & Dağlar, 2016; Breetzke & Cohn, 2013; Choi, 2008; Groff, 2007; Holtfreter, Reisig, & Pratt, 2008; Kigerl, 2012; Louderback & Roy, 2018; Mustaine, & Tewksbury, 1998; Spano, & Nagy, 2005; Tewksbury, & Mustaine, 2000). For a majority of motivated hackers, financial gain is still the primary and ultimate goal through the phishing process or by installing malware to obtain data and information from victims. Also, financial institutions and users may not be able to stop motivated offenders as RAT assumes, because we are less likely to know where and who these criminals are until after they commit an offense. It can be argued that without capable cyber guardianship, the odds of network penetration and victimization will not only increase but so will the opportunity for an offender's escape in cyberspace (Jaishankar, 2008).

The costs incurred with offenses such as the current case are not limited to the direct costs of money stolen. On the day of the incident, the FCB froze 1,000 ATMs and stopped the service of withdrawals which no doubt cost the public and general commerce significant inconveniences. These costs could be considered secondary losses from the overdrawn ATMs (see Anderson et al., 2013). After the investigation, it was determined that approximately 4 percent of the 27,200 machines in their ATM network in Taiwan might have been affected by the cyber-attack and needed further inspection (Reuters, 2016). Also, the system and software of the FCB in Taiwan may have to be upgraded and additional training provided to encourage employee awareness measures. These consequences represent additional defensive costs. In addition, the hacking incident could possibly undermine citizen confidence in the bank and online banking in general as well as damage the image and reputation of financial service institutions; all of which can be considered indirect costs. The direct and indirect costs to society of hacking incidents such as these are not easy to accurately estimate as Anderson and associates (2013) indicate, however their impact on individuals, organizations, the criminal justice system and the society as a whole would be substantial. Thus the current study offers some policy implications to improve cyber security and cyber crime control.

First, institutions have to keep their operating system and basic software up to date and keep upgrading and *enhancing computer physical defense systems* such as installing anti-virus software, using firewalls and email spam filtering, malware detection, securing browsing, networking activities monitoring and patching potential threats of bugs and holes. While implementing network security may be costly, there is no magic number that one should spend to reach and maintain adequate levels of security that ensure a hack-free system. Realistically, a company should find the balance between cost or affordability and the processes necessary to maintain guardianship against data breaches and system compromises.

Second, an enterprise should work with IT special consultants and cyber security mangers and *develop guidelines that address prevention and defenses, as well as a response and recovery plan. Businesses should hold user cyber security training* to protect their intranet and internet at all employee and administrative levels. This plan should be able to provide basic cyber security knowledge to users within the company and prevent cyber security negligence. The defense system should assess and detect data or network breaches, virus infections or any security threats at their initial stages. With periodic internal users' training and system drilling, the enterprise should be able to respond with appropriate

strategies to stop cyber vulnerability and minimize potential losses. After identifying attacks, the company should be able to conduct damage control and assessment as well as implement approaches to recover system losses and to repair the affected network and system. Furthermore, they should hold cyber security meetings routinely to update relevant members about cyber security and prevention plans.

Third, given increasing trends toward the use of electronics in daily life, cyber crime and victimization may occur more often merely because more individual devices are connected to the Internet (Singer & Friedman, 2013). Consequently, *strengthening non-work place personal guardianship* is critical for preventing victimization. As expected, work place related network and computer security policies are more stringent than non-work places and may help to restrain individual online behaviors (Williams, 2016). However, online users in non-work place settings (e.g. homes, restaurants, airports, cafés) may have more unprotected exchanges which increase the odds of being victimized in cyberspace. In non-work settings, users should not plug-in thumb drives without encryption; activate unsecured devices to browse websites, nor update computer software frequently, using passwords that are easy to guess. In addition, they should avoid having inappropriate security settings and arbitrarily downing free files and installing downloaded applications that may contain undetected malware.

Fourth, although cyberspace has been viewed as a virtual space with "zero distance" between all points that does not mean that crime "hotspots" cannot be located there as it is in physical space like street corners or parks. An IP address in cyberspace can be viewed much like locations in the physical environment and one could even pin point a certain machine with a permanent or temporary address where it can be exploited by offenders in cyberspace. Therefore, *changing user's online risky behaviors* through re-education on security and *making people aware of the threats of cyber victimization* could also enhance cyber crime prevention. Users should be aware that certain online activities, for instance, spending too much time online shopping and banking, watching pictures and videos that may have contain malware, playing video games, downloading music and media that may have viruses, and accessing social media, chatting in online rooms, forums and chat boxes would disproportionately increase their online visibility. Subsequent interaction with potential offenders would expose them to the risk of becoming a suitable target in cyberspace.

And finally, we need more research on different cases to understand types of cyber crime and cyber victimization in order to become more effective both formally and informally with mechanisms to prevent potential cyber crime threats. Even though this may be very difficult to do given the nature of cyberspace where deterrence may be harder to achieve, enhancing social and community cohesion may reduce some high risk behaviors. As Jaishankar (2008) posits, cyber crime may be reduced with more self-regulation, bounded by integrity and honesty as reflected in moral standards and ethical principles. Enhancing civic virtue, responsibly and the expectations of being law-abiding citizens may alleviate some of the root causes of not only cyber crime but also all other types of crime as well.

Limitations

The current case study extends the theoretical framework of RAT to the domain of the victimization of financial institutions and provides another piece of evidence indicating that such an approach can be a useful framework for understanding the victimization of

financial institutions involving hacking. Still, it may be argued that the case study method does not use conventional statistical analysis as prior studies have (Argun, &Dağlar, 2016; Breetzke & Cohn, 2013; Holtfreter et al., 2008; Louderback & Roy, 2018; Mustaine, & Tewksbury, 1998) and is a less reliable form of evidence for theorizing about cyber criminology. However, the current study is still valuable and contributes to the field for a number of reasons. First, none of prior studies examined cyber ATM hacking and little is known about this type of cyber victimization. Given a subsequent high-profile ATM jackpotting heist activity in the Unites States (Volz, 2018), the current case study sheds light on the modus operandi of ATM hacking as well as the factors that may be associated with elements of RAT in a virtual environment. Second, although cases of cyber ATM hacking are relatively rare compared to other types of cyber crime such as phishing, spam identify theft, and fraud, they may involve substantial sums of money and risk undermining a common commerce function that most people participate in. Third, this is not just a national case for Taiwanese authorities but also an international case worthy of attention regarding modus operandi and prevention of ATM hacking (Sancho et al., 2017). This analysis may be useful for theorizing about organized crime, comparative criminal justice and computer software design. Given the current study's limitations as a case study based on qualitative interviews, more research is needed to better understand cyber ATM hacking. After cumulating enough cases, we may further examine this type of victimization by using quantitative approaches.

Although the applicability of RAT might be limited in cyber crime due to spatio-temporal disorganization and the argument that it is not easy to demonstrate how cyber criminals and victims "converge in space and time" as noted by Yar (2005, p. 424), the current study using the broader doctrine of RAT found support for the essence of RAT particularly the three basic elements of crime. These findings are consistent with prior studies in cyber criminology (Argun, & Dağlar, 2016; Breetzke & Cohn, 2013; Holtfreter et al., 2008; Louderback & Roy, 2018; Mustaine, & Tewksbury, 1998). Future study should continue to explore how routine activities theory could be applied to cyberspace or even whether or not to develop other theoretical explanations about cyber victimization.

Applying the elements of RAT might be a simplistic conceptualization of cyber crime; however, as discussed above, its applicability was supported by the current case study and other prior quantitative studies analyzing larger victimization databases. Moreover, analyzing this FCB case in a RAT framework would helps us to understand particular patterns in offending over time and cyberspace that could not be tracked by aggregated victimization data. The current case study further allows crime prevention specialists to design strategies that could specifically address cyber offender behavior, reducing motivation and increasing deterrence in the near future. Or, efforts could focus on potential targets, educating and engaging victims in protection as well as risk avoidance. And finally, resources could be directed at determining which options would be the most effective for the use of a wide range of guardians or guardian-like instruments). All of these strategies are consistent with the framework of RAT.

References

Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M. J. G., Levi, M., et al. (2013). Measuring the Cost of Cyber crime. In R. Böhme (Ed.), *The economics of Information security and privacy* (pp. 265-300). Berlin, Heidelberg: Springer.

Antonescu, M., & Birău, R. (2015). Financial and non-financial implications of cyber crimes in emerging countries. *Procedia Economics and Finance, 32*, 618-621.

Argun, U., & *Dağlar*, M. (2016). Examination of Routine Activities Theory by the property crime. *International Journal of Human Sciences, 13*(1), 1188-1198.

Bossler, A. M., & Holt, T. J. (2009). On-line activities, guardianship, and malware infection: An examination of Routine Activities Theory. *International Journal of Cyber Criminology, 3*(1), 400-420.

Breetzke, G. D., & Cohn, E. G. (2013). Burglary in gated communities: An empirical analysis using routine activities theory. *International Criminal Justice Review, 23*(1), 56-74.

Britz, M. (2013). *Computer Forensics and Cyber Crimes: An Introduction (3rd edition)*. Upper Saddle River, NJ: Pearson Education Inc.

Castells, M. (2002). *The Internet galaxy: Reflections on the Internet, business, and society*. Oxford: Oxford University Press.

Choi, K.-S. (2008). Computer crime victimization and integrated theory: An empirical assessment. *International Journal of Cyber Criminology, 2*, 308-333.

Cohen, L. E., &Felson, M. (1979). Social change and crime rate trends: Routine activity approach. *American Sociological Review, 44*(4), 588-608.

Cybersecurity Ventures. (2017). *2017 cyber crime report*. Menlo Park, CA: Cybersecurity Ventures.

Danquah, P., & Longe, O. B. (2011). An empirical test of the Space Transition Theory of cyber criminality: Investigating cyber crime causation factors in Ghana. *African Journal of Computing and ICTs, 44*(2), 37-48.

Eck, J. E., & Clarke, R. V. (2003). Classifying common police problems: A routine activity approach. *Crime Prevention Studies, 16*, 7-39.

Eisenstein, J., & Jacob, H. (1977). *Felony justice: An organizational analysis of criminal courts*. Lanham, MD: University Press of America.

Federal Bureau of Investigation. (2017). *2016 Internet crime report*. Washington, DC: Federal Bureau of Investigation.

Finkle, J., & Wu, J. R. (2017, January 4). Taiwan ATM heist linked to European hacking spree: Security firm. Reuters. Retrieved from https://www.reuters.com/article/us-taiwan-cyber-atms/taiwan-atm-heist-linked-to-european-hacking-spree-security-firm-idUSKBN14P0CX.

Grabosky, P. (2001). Virtual Criminality: Old Wine in New Bottles? *Social and Legal Studies, 10*(2), 243-249.

Groff, E. R. (2007). Simulation for theory testing and experimentation: An example using routine activity theory and street robbery. *Journal of Quantitative Criminology, 23*(2), 75-103.

Hawley, A. (1950). *Human ecology: A theory of community structure*. New York, NY: Ronald.

Hinduja, S. (2001). Correlates of internet software piracy. *Journal of Contemporary Criminal Justice, 17*, 369-382.

Holt, T. J., & Bossler, A. M. (2009). Examining the applicability of lifestyle-routine activities theory for cyber crime victimization. *Deviant Behavior, 30*, 1-25.

Holt, T. J., & Bossler, A. M. (2013). Examining the relationship between routine activities and malware infection indicators. *Journal of Contemporary Criminal Justice, 29*(4), 420-436.

Holt, T. J., & Bossler, A. M. (2014). An assessment of the current state of cyber crime scholarship. *Deviant Behavior, 35*, 20-40.

Holtfreter, K., & Meyers, T. J. (2015). Challenges for cyber crime theory, research, and policy. In G. C. Lajeunessehe (Ed.), *Norwich review of international and transnational crime* (pp. 54-66). Norwich, VT: The Program of International and Transnational Crime.

Holtfreter, K., Reisig, M. D., & Pratt, T. C. (2008). Low self-control, routine activities, and fraud victimization. *Criminology, 46*(1), 189-220.

Hsieh, C.-L., Chien, L.-C., Chen, W.-T., Wang, M.-L., Lu, K.-C., & Chang, W.-C. (2016, September 14). 一銀盜領案, 3外嫌被求刑12年 [First Commercial Bank heist case: The prosecution asked for 12 years for three arrested suspects]. *Liberty Times*.
Retrieved from http://news.ltn.com.tw/news/focus/paper/1031930.

Hutchings, A., & Hayes, H. (2009). Routine activity theory and phishing victimization: Who got caught in the 'net'? *Current Issues in Criminal Justice, 20*, 432-451.

International Telecommunication Union. (2016). *Measuring the information society report: 2016*. Geneva, Switzerland: International Telecommunication Union.

Jaishankar, K. (2008). Space Transition Theory of cyber crimes. In F. Schmalleger & M. Pittaro (Eds.) *Crimes of the Internet* (pp. 283-301). Upper Saddle River, NJ: Prentice Hall.

Kigerl, A. (2012). Routine activity theory and the determinants of high cyber crime countries. *Social Science Computer Review, 30*(4), 470-486.

Leukfeldt, E. R. (2014). Phishing for suitable targets in the Netherlands: Routine activity theory and phishing victimization. *Cyberpsychology, Behavior and Social Networking, 17*(8), 551-555.

Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cyber crime: A theoretical and empirical analysis. *Deviant Behavior, 37*(3), 263-280.

Levi, M. (2017). Assessing the trends, scale and nature of economic cyber crimes: Overview and issues. *Crime, Law and Social Change, 67*, 3-20.

Louderback, E. R., & Roy, S. S. (2018). Integrating social disorganization and routine activity theories and testing the effectiveness of neighborhood crime watch programs: Case study of Miami-Dade county, 2007-15. *British Journal of Criminology, 58*(4), 968-992.

Marcum, C. D., Higgins, G. E., & Ricketts, M. L. (2010). Potential factors of online victimization of youth: An examination of adolescent online behaviors utilizing routine activity theory. *Deviant Behavior, 31*(5), 381-410.

Mitnick, K. D. & Simon, W. L. (2001). *The art of deception: Controlling the human element of security*. John Wiley & Sons.

Mustaine, E. E., & Tewksbury, R. (1998). Predicting risk of larceny theft victimization: A routine activity analysis using refined lifestyle measures. *Criminology, 36*(4), 829-858.

Ngo, F. T., & Paternoster, R. (2011). Cyber crime victimization: An examination of individual and situational level factors. *International Journal of Cyber Criminology, 5*, 773-793.

Paek, S. Y., & Nalla, M. K. (2015). The relationship between receiving phishing attempt and identity theft victimization in South Korea. *International Journal of Law, Crime and Justice, 43*, 626-642.

Poushter, J. (2016). *Smartphone ownership and Internet usage continues to climb in emerging economies*. Washington, DC: PEW Research Center.

Pratt, T. C., Holtfreter, K., & Reisig, M. D. (2010). Routine online activity and internet fraud targeting: Extending the generality of routine activity theory. *Journal of Research in Crime and Delinquency*, 47, 267-296.

PWC. (2014). *Threats to the financial services sector*. UK, London: PricewaterhouseCoopers LLP.

PWC. (2016). *Adjusting the lens on economic crime: Preparation brings opportunity back into focus*. UK, London: PricewaterhouseCoopers LLP.

Reisig, M. D., & Holtfreter, K. (2013). Shopping fraud victimization among the elderly. *Journal of Financial Crime*, 20, 324-337.

Reuters. (2016, July 17). Taiwan says foreign suspects arrested over $2 million ATM cyber robbery. Reuters. Retrieved from https://www.reuters.com/article/us-taiwan-banks-theft/taiwan-says-foreign-suspects-arrested-over-2-million-atm-cyber-robbery-idUSKCN0ZX0N7.

Reuters. (2017, December, 12). Taiwan's Far Eastern International fined T$8 million over SWIFT hacking incident. Retrieved January 7, 2018, from https://www.reuters.com/article/us-far-eastern-fine/taiwans-far-eastern-international-fined-t8-million-over-swift-hacking-incident-idUSKBN1E60Y3.

Reynald, D. M. (2010). Guardians on guardianship: Factors affecting the willingness to monitor, the ability to detect potential offenders and the willingness to intervene. *Journal of Research in Crime & Delinquency, 47*, 358-390.

Reyns, B. W. (2013). Online routines and identity theft victimization: Further expanding routine activity theory beyond direct-contact offenses. *Journal of Research in Crime and Delinquency, 50*(2), 216-238.

Reyns, B. W. (2015). A routine activity perspective on online victimization: Results from the Canadian general social survey. *Journal of Financial Crime, 22*(4), 396-411.

Reyns, B. W., Henson, B., & Fisher, B. S. (2011). Being pursued online: Applying cyberlifestyle-routine activities theory to cyberstalking victimization. *Criminal Justice and Behavior, 38*(11), 1149-1169.

Rogers, M. K. (2001). *A social learning theory and moral disengagement analysis of criminal computer behavior: An exploratory study*. Unpublished doctoral dissertation, Manitoba University, Canada.

Sancho, D., Huq, N., & Michenzi, M. (2017). *Cashing in on ATM malware: A comprehensive look at various attack types*. Retrieved from https://documents.trendmicro.com/assets/white_papers/wp-cashing-in-on-atm-malware.pdf.

Singer, P. W., & Friedman, A. (2013). *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press.

Soudijn, M. R. J., & Zegers, B. C. H. T. (2012). Cyber crime and virtual offender convergence settings. *Trends in Organized Crime, 15*, 111-129.

Spano, R., & Nagy, S. (2005). Social guardianship and social isolation: An application and extension of lifestyle/routine activities theory to rural adolescents. *Rural Sociology, 70*,

414-437.

Taipei District Prosecutors Office. (2016). *Press release*. Taipei District Prosecutors Office.

Taylor, R. W., Caeti, T. J., Loper, D. K., Fritsch, E. J., & Liederbach, J. (2006). *Digital crime and digital terrorism*. Upper Saddle River, NJ: Pearson Prentice Hall.

Tewksbury, R. & Mustaine, E. E. (2000). Routine activities and vandalism: A theoretical and empirical study. *Journal of Crime and Justice, 23*(1), 81-110.

vanWilsem, J. (2013). 'Bought it, but never got it': Assessing risk factors for online consumer fraud victimization. *European Sociological Review*, *29*(2), 168-178.

Volz, D. (2018, January 29). "Jackpotting" hackers steal over $1 million from ATMs across U.S.: Secret Service. *Reuters*. Retrieved from https://www.reuters.com/article/us-usa-cyber-atm/jackpotting-hackers-steal-over-1-million-from-atms-across-u-s-secret-service-idUSKBN1FI2QF.

Williams, M. L. (2016). Guardians upon high: An application of routine activities theory to online identity theft in Europe at the country and individual level. *British Journal of Criminology, 56*, 21-48.

Wooldredge, J. D., Cullen, F. T., & Latessa, E. J. (1992). Research note victimization in the workplace: A test of routine activities theory. *Justice Quarterly, 9*(2), 325-335.

Yar, M. (2005). The novelty of cyber crime: An assessment in light of routine activity theory. *European Journal of Criminology, 2*(4), 407-427.