SciDoc Publishers
Infer, Interpret & Inspire Science

International Journal of Forensic Science & Pathology (IJFP)
ISSN 2332-287X

Ransomware Against Police: Diagnosis of Risk Factors via Application of Cyber-Routine Activities Theory

Research Article

Choi KS[1,2*], Scott TM[2], LeClair DP[2]

[1] Bridgewater State University, Massachusetts, USA.
[2] Boston University, Massachusetts, USA.

Abstract

Technologically advanced hackers are able to commit a crime and leave undiscovered by the authorities. Recent increases in cyber-attacks utilizing technology known as ransomware are leaving police departments and other institutions in the serious situation of having to pay ransom to cybercriminals. The present study employs a Cyber-Routine Theoretical approach in explaining why ransomware victimization has become a viral phenomenon. Data were derived from the recent reported cases of ransomware attacks towards police departments in the US. and analyzed in order to build a victim profile. This study shows that online lifestyle and cybersecurity are the salient factors that contribute to the ransomware victimization. Future potential preventive measures and policies will be discussed.

Keywords: Ransomware; Cyber-Routine Activities Theory; Computer Crime Victimization; Online Lifestyle; Cybersecurity.

Introduction

As technology evolves, online users are facing more substantial threats and constantly encountering new forms of extortion via cyber attacks. Currently, a more advanced and less detectable form of extortion is riddling the nation; it is called ransomware. Cybercriminals are able to capture other computer users' data and demand a ransom in order for its return. Ransomware is a form of malware that encrypts all of the data on a user's computer device and network, then denies the user access to the device until a ransom has been paid [1]. Recent ransomware is capable of encrypting files on a shared network system, which can essentially disable an entire organization's data.

Cybercriminals often hide ransomware programs such as KEYHolder, CryptoLocker, and CryptoWall in attachments or hyperlinks contained in emails. Once the user clicks on the attachment or hyperlink, the malicious attack occurs. Documents, programs, and applications on the victim's computer become encrypted, and the ransom amount with instructions, along with a deadline, appears on the computer screen [1].

Ransomware originated in 1989 with the program known as AIDS Trojan [1]. AIDS Trojan lacked the sophistication of the contemporary types of ransomware due to the fact that most people did not use personal computers, nor was the internet nearly as popular in late 1980 and early 90s [1]. It was not until 2005 that ransomware cases became an imminent issue. In Russia, cases of ransomware were initially more often reported along with ample monetary loss [2]. Since 2005, ransomware has repeatedly evolved by adding social engineering techniques and advanced encryption technology [1]. Once CryptoLocker was released in 2013, cybercriminals using ransomware tended to increase ransom amounts while widely infecting computers and networks in both private and public sectors [1]. Within a few months of CryptoLocker's release, more than $27 million in ransom payments were made [3]. According to the Internet Crime Complaint Center, the release of a new ransomware program, CryptoWall, garnered criminals over $18 million from April 2014 through June 2015 [4]. Currently, the number of ransomware victimization in the first quarter of 2016 has increased by 3,500% when compared to the fourth quarter of 2015 [5].

Cybercriminals will often demand their ransom be paid in bitcoins. Bitcoins are a virtual currency, the transactions of which are recorded as addresses that are not tied into an individual's

***Corresponding Author**:
Kyung-shick Choi
Department of Criminal Justice, 10 Shaw Road, Bridgewater State University, Bridgewater, MA 02325, USA.
Tel: 617-358-2807
E-mail: kchoi@bridgew.edu

Received: June 22, 2016
Accepted: July 18, 2016
Published: July 23, 2016

Citation: Choi KS, Scott TM, LeClair DP (2016) Ransomware Against Police: Diagnosis of Risk Factors via Application of Cyber-Routine Activities Theory. *Int J Forensic Sci Pathol.* 4(7), 253-258. **doi:** http://dx.doi.org/10.19070/2332-287X-1600061

identity nor governed by traditional banking systems, therefore making the transaction essentially anonymous [6]. In addition to bitcoin payments, cybercriminals demand the victim to pay via Darknet sites, which increase their anonymity even more. Demanding bitcoins as a ransom payment method enables the transaction to occur over an anonymizing internet browser such as TOR (The Onion Router), which is a special network encryption browser for hiding all the origination and ending destination for the traffic [7]. Cybercriminals demand their victims to download TOR to complete the payment transaction, which easily allows them to evade law enforcement detection.

In recent years, cybercriminals mainly target public industries including hospitals, municipal departments, town officials, and police departments. Police departments are one of the major targets of this hostile attack. The most recent case of ransomware within a police department occurred in Massachusetts. On the evening of February 25, 2016, an email was sent to every member of the police department. Within the email was an arcane maliciousness, ransomware. Once a member of the department opened the email, the ransomware began encrypting files in the police department's network and seized complete control over one of their major pieces of software, TriTech [8]. TriTech is an essential police software which allows officers to log incidents during shift and facilitates dispatching operations. The cybercriminal using ransomware demanded to be paid one bitcoin (Approximately 450 dollars) in return of the encrypted files.

Another local police department in Massachusetts experienced a similar malevolent crime. The police network started to become slow and inconsistent for a short period of time, and then a message popped up onto computer screens in the department reading "Your personal files are encrypted. File decryption costs $500" [9]. The police chief of the department attempted to decrypt the files without paying the ransom with assistance from federal and state agencies as well as two private cyber security firms [9]. The encryption from the ransomware proved too challenging to be solved by these combined efforts, resulting in the police department paying the ransom five days later.

Despite the growth and prevalence of ransomware attacks, criminological examinations explaining such a viral-phenomenon have not yet been applied. The purpose of this study is to focus on analyzing the emergence of ransomware attacks against police departments in the U.S. and conveying a detailed victimization profile of police departments facing ransomware attacks. In other words, the reported ransomware against the police departments will be examined using Cyber-Routine Activities Theory (C-RAT), which can diagnose the risk factors of ransomware victimization. Upon presenting a theoretical overview of the cyber-routine activities theory, while emphasizing how the main theoretical elements, online lifestyle and cybersecurity, can be applied to the ransomware attack cases, a review of the relevant literature will be presented. This section will then be preceded by a presentation of the research methodology and data analysis. Finally, the study will discuss the main findings and potential policy implications, along with a discussion of study limitations and future implications.

Cyber-Routine Activities Theory

Cyber-routine activities theory embraces Cohen and Felson's traditional RAT (Routine Activities Theory) as a new theoretical application for primarily explaining computer crime victimization. Cohen and Felson proposed the RAT theory in 1979 concerning three main tenets: motivated offenders, suitable targets, and absence of capable guardians [10] for examining traditional crime victimization. RAT has been widely applied as a situational crime prevention strategy to 'reduce opportunities for specific categories of crime by increasing the associated risks and difficulties and reducing the rewards' [10]. Thus, the absence of any one of the tenets would prevent crime occurrence [10].

While the three factors Cohen and Felson posited have been found useful in preventing a variety of situational traditional crimes and used extensively in testing for numerous forms of crime, it is difficult to use it to examine the forms of cybercrime and computer crime victimization. The motivated offender tenet suggests that there will always be an infinite amount of crime motivation. In fact, ransomware attacks have proven to be a successful monetary opportunity for cybercriminals. According to CNN News (2016), ransomware has collected $209 million dollars within the first few months of 2016 [11]. Ransomware allows cybercriminals to withhold valuable data from users' and agencies' computers until a ransom has been paid with relative ease and anonymity. Thus, Cyber-routine activities theory (2008) also crosses parallels with Cohen and Felson's argument in highlighting motivated offenders as a given situational factor [6].

Choi (2008) argues that the suitable target tenet in respect to cyberspace is also a given situational factor [6]. Felson (1998) used four properties to assess the suitable target tenet, commonly referred as VIVA (value, inertia, visibility, and accessibility) [6]. Choi (2008) also argues that any user accessing the internet is viewed as a valuable target with a perfectly high vulnerability to a cybercriminal [12]. For example, when the victims' data are seized from the ransomware, the victims tend to pay the ransom because they are essentially powerless in retrieving important files and data.

In terms of capable guardianship, there is a conspicuous lack of capable formal guardianship in ransomware cases. Formal social controls are agencies in the criminal justice system [6]. Choi argues that the current formal social agents do not provide effective safeguards to protect potential victims in cyberspace since the amount of specialized forces responsible for patrolling cyberspace are limited due to the lack of resources and training [6]. As a result, the police departments encountering ransomware incidents tend to pay the ransom without making any arrests. This substantially weakens the level of capable guardianship, imposing a negative image of the police departments' capability in handling these cases. Citizens can foster feelings of distrust and fear if the police of their town are unable to stop cybercriminal activities, let alone kowtowing to criminals by paying them. Furthermore, the FBI has done little to suggest there is a way to retrieve the encrypted information without paying the ransom. Although the FBI publicly states on their webpage that they do not condone paying ransom, an individual agent admits to the contrary. An FBI agent stated at a conference that "the ransomware is that good, to be honest, we often advise people just to pay the ransom" [13]. Furthermore, jurisdictional issues also contribute to a lack of capable guardianship. Perpetrators of ransomware could be located anywhere in the world. Collaboration with global nations to provide international cooperation in the investigation of ransomware is extremely challenging [6]. Therefore, the concept of Cohen and

Felson's RAT theoretical application falls in line with the limited scope of situational crime prevention in cyberspace.

Choi (2008) proposed Cyber-Routine Activities Theory (Cyber-RAT) via integration of Hindelang's lifestyle exposure theoretical perspective with the concept of Cohen and Felson's capable guardianship [6]. According to Choi (2008), there are two risk factors that contribute to computer crime victimization: 1) online lifestyle and 2) lack of cybersecurity. The tenet suitable target is represented as online lifestyle in Choi's (2008) cyber-routines activities theory. A number of researchers have found an empirical connection between risky online behavior and cybercrime victimization [6, 12, 14]. Choi (2008) posits that individuals' vocational and leisure activities play a larger role in determining computer crime victimization than controlling constant criminal motivation in cyberspace. Thus, the level of individuals' risky online behaviors are one of salient factors, which substantially contributes to computer crime victimization and makes them a suitable target. In this study, the focus is primarily on police officers' vocational activities because the ransomware infected the computer systems and networks during police work hours. Vocational activities in these situations can consist of police officers opening emails and browsing the web during their shifts. Users' online lifestyle is central to falling prey to computer crime victimization. When users frequently visit unknown websites, illegally download files, or open hyperlinks in emails that are unfamiliar to them, it increases the likelihood of computer crime victimization [12]. In other words, inadequate care in online lifestyle increases human error, which contributes to a cause of ransomware victimization. Human error transpires when an online user clicks an attachment in the form of a hyperlink contained in an email. Other causes of ransomware attacks tie into risky downloading behavior such as downloading free versions of software such as cracked versions of games, adult content, screensavers or movies, etc.

Choi (2008) revised the traditional RAT component of capable guardianship by replacing the concept with cybersecurity, called *Digital Capable Guardianship*, which is the most viable tenet in the cyber-routine activities theory. Cybercriminals are scrupulous in their efforts to advance ransomware. Each year, ransomware programs become more technologically advanced and substantially more damaging to their victims. In 2013, CryptoLocker was released and had the ability to encrypt files on a computer system. CryptoWall was released in 2014 and was able to perform the same function, but with the addition of encrypting other devices connected to the first target computer [1]. KeRanger has been active since March of 2016; this ransomware is the first to target the OS X (Mac Computer Systems) operating system. KeRanger combines a time bomb function which waits a certain period of time before encrypting all the data of Mac computer systems as well as devices connected to the computer [15]. Another recent type of ransomware, Peyta Ransomware, released in 2016, aims to block the entire hard drive by controlling the Master Boot Records and Master File Table. The Master Boot Records contain all of the data and a specific code for booting the operating system (OS) [16]. Once Peyta Ransomware infects the computer, it disrupts the booting system, rendering the hard drive inaccessible [16]. The functions and capabilities of newly released ransomware constantly evolve and inflict more harm to computer networks and systems. The attacks are more sophisticated, which make keeping up with the most advanced cybersecurity crucial. Therefore, utilizing the most updated and effective cybersecurity plays a pivotal role in keeping computer system safe from ransomware attacks.

Methodology

Sample and Property of Measures

The data were derived from the reported ransomware cases targeting police departments from the years 2013 to May 2016. We verified information from social media and news outlets and reaffirmed with the police departments via communicating through social media network sites. The collected data consists of 1) date of victimization, 2) victim states, 3) size of police department, 4) ransom amount, 5) whether or not the police department paid the ransom, and 6) the method of ransomware that attacked the computer system and network and the content within the ransomware i.e., phishing attacks, spear phishing attacks or digital fax. General descriptive statistics were taken regarding the sample.

Dates of Reported Cases: The data indicate that the number of ransom attacks targeting police departments has dramatically increased from 1 incident to 8 incidents between 2013 and 2015. The rate of change was an 800% increase from 2013 to 2015 (See Figure 1).

Victim States: The data indicate that Ransomware attacks occurred in 6 different states (Alabama, Illinois, Massachusetts, Maine, New Hampshire, and Tennessee). There were 11 local police departments and 2 sheriff departments affected in this study. There were 13 ransomware cases in total, affecting all different police departments. Maine and Massachusetts police departments experienced the most amount of ransomware attacks; Maine endured 6, and Massachusetts confronted 3 (See Figure 2).

Size of Police Department: Size of police department was determined through searching the official police department's webpage and messaging the departments via social media. This study includes all officers (i.e. part-time, full-time, reserve police officers) of the department. The average size of police department including full-, part-time and reserve officers is 27 police officers. The average for only full-time police officers in this study is 24.6. The police departments ranged from the maximum staffed officers (58) to the minimum staffed officers [7]. The largest police department was in Massachusetts, which staffed (58). The original responses on size of police department were coded to a scale from 1 to 5 (1 = 1-10, 2 = 11-20, 3 = 21-30, 4 = 31-40, 5 = 41-60). The mean score of police department size for this sample is 3 (21-30 officers), with a standard deviation of 1.47, a skewness of .19, and a kurtosis of -1.401.

Ransom Amount: This study includes the ransom amount demanded from the ransomware attacks as an important variable as well. The mean of ransom amount for this sample is 415.64 (The U.S. dollar amount), with a standard deviation of 152.28, a skewness of 1.15, and a kurtosis of .699. (See Figure 3).

Ransom Paid by Police & Method of Ransomware Attack

Data indicate that 85% (11 out of 13 cases) of police departments paid the ransom via the Bitcoin payment system. All the attacks were derived from emails containing hyperlinks and attachment,

Figure 1. Dates of Reported Cases.

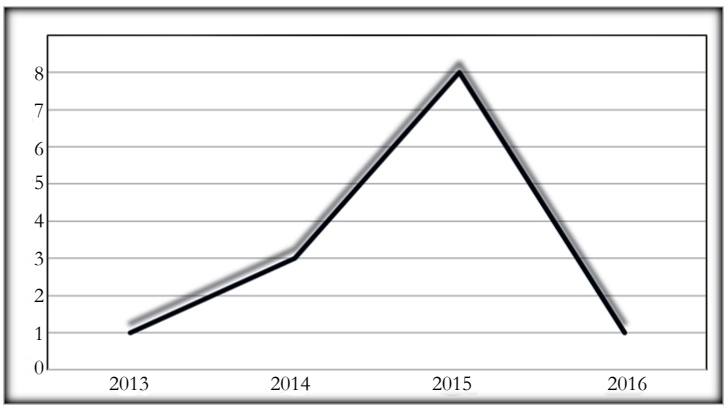


Figure 2. Victim States.

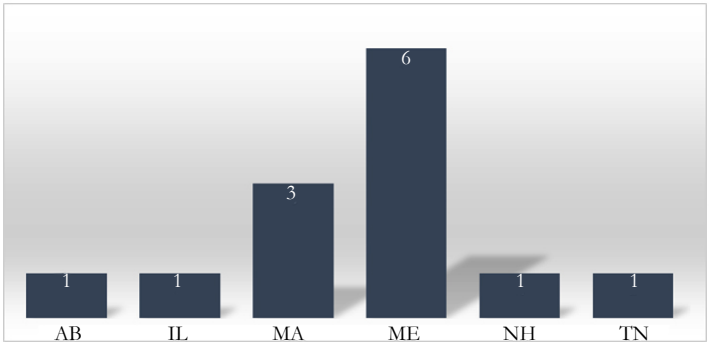
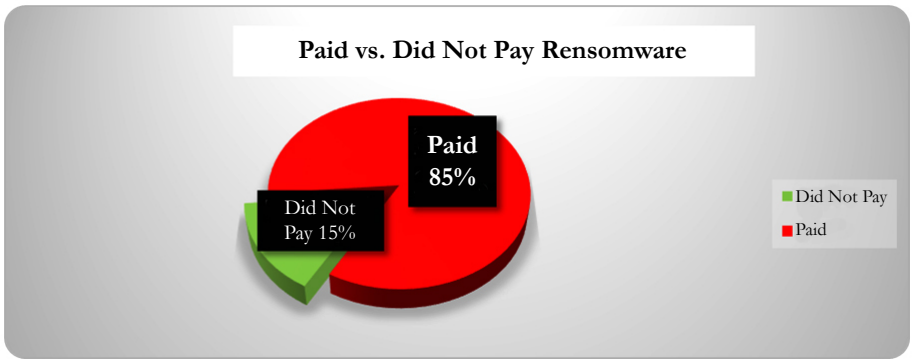


Figure 3. Paid v. Did Not Pay Ransomware.



which infects data encryption.

Analysis of Ransomware Incidents against Police Departments: Cyber-RAT Approach

Motivated Offender

As previously addressed in the literature, there are varying levels of offender motivation that impact a potential crime occurrence. Thus, 'situational motivation' plays a significant role in determining criminal activity. The results indicate that a situational motivation of cybercriminals for attacking police departments is linked to the size of the police department.

The research examined the statistical relationship between police department size and ransom amount. In order to examine whether police department size has a substantial impact on the level of ransom amount, Ordinary Least Squares (OLS) regression analysis was applied.

The unstandardized coefficients of 76.85 indicated that the department size has positive, substantial impacts on the level of ransom amount ($p. <.05$). This result suggests that police departments of a larger size are more likely to be informed the larger amount of ransom payment request from cybercriminal (See Table 1). Based on the R-Square, 55% of the variation in the ransom amount can be explained by department size difference (see Table 1). There is a moderate to strong, positive significant relationship between department size and the level of ransom amount. In other words, the larger the police department, the larger the ransom amount the ransomware demanded. Likewise, the smaller the department, the smaller the ransom payment was demanded. The results suggest that cybercriminals may know about their specific

target since the ransom amount was determined by size in order to maximize their chances of getting the ransom paid. In fact, smaller police departments lack the funds and resources to pay highly expensive ransom amounts, whereas larger departments have resources and funds available and are therefore able to afford higher ransom payments.

Profiling the type of hacker responsible for ransomware is pertinent to this research. NBC News has stated most of the ransomware viruses originated in Russia and other Eastern European countries [17]. 12% of the hosts, in 2016, for ransomware programs are in Russia [5]. It is also important to note that the first effective ransomware programs released in 2005 were reported only in Russia [2]. According to Shoemaker and Kennedy (2009), a ransomware attacker could be tied into the Mafia Soldier within the cybercriminal typology. The Mafia Soldier is motivated through monetary gains with the intention of theft, extortion and invasion of privacy for the purposes of blackmail. They tend to target specific victims and understand the importance of data associated with the victims' computer system. This fits the model for ransomware due to its extortion methodology and invasion of privacy. The description of this offender can range from any age, and is typically an organized crime member operating out of the Far East or Eastern Europe [6].

Online Lifestyle

As previously discussed, this study confirms the ransomware attacks were all executed through means of an email. The exact form the ransomware used to take over the police departments' computer systems and networks were through emails. 92.3% of the cases related to clicking hyperlinks in the email contents and 7.7% of the cases related to opening digital fax were found in the case analysis. This finding suggests that cybercriminals targeting police departments activated spear phishing tactics to infect the computer systems and networks with ransomware because the attacker knew which departments they are specifically targeting. The ransomware case in NH reaffirms this finding. According to the incident report, a police officer opened a digital fax attached in an email about an investigation the officer was working on. However, the digital fax was actually the ransomware the cybercriminal cultivated in the malicious email [18]. In sum, cybercriminals operating ransomware attacks understand their targets' vocational activities and purposely send very personalized emails containing attachments or hyperlinks embedded with malicious ransomware.

Digital Capable Guardianship: Cybersecurity

In regards to cases of ransomware, police departments who have been equipped with up-to-date cyber security and regularly back up all their files are less likely to become targets. Only 15% (2 out of 13 cases) of the police departments in this study did not pay the ransom demanded by the ransomware, whereas 85% of the police departments did. One local one police department in New Hampshire did not succumb to paying the ransom because they were able to reacquire a large portion of their files due to the presence of a secure backed up system [17].

In most cases, police departments were equipped with minimal cybersecurity and did not utilize a backup system. The police department in Alabama lost all of their essential data when the ransomware infected their computer system and network because they refused to pay the ransom and did not have a backup system to store their data in addition to lacking adequate cybersecurity [17]. A police department in MA had computers that operated on DOS, an outdated disc operating system, and lacked up to date backups of its files [9, 17]. Inevitably, the department had to pay the ransom in order to retrieve its data. The consequences of having inadequate cybersecurity and not routinely running backups of important data is having to resort to pay the ransom in order to retrieve the data back.

In sum, departments leaving a computer unprotected with inadequate cybersecurity are more susceptible to ransomware attacks. Regularly changing passwords to secure the computer network and system greatly strengthens their protection against ransomware attacks. Using the most updated version of cyber security with a secure systematic back-up system plays an important role in minimizing ransomware victimization.

Discussion and Conclusions

This study assessed the recent ransomware attacks targeting police departments to construct a victim profile and its preventive measures via Choi's (2008) cyber-routine activities theory. The central findings indicate that online lifestyle and digital-capable guardianship (cybersecurity) directly influence ransomware victimization.

Police departments without proper awareness of their vocational online activities are likely to become victims of ransomware. Particularly, department staff/officers who download attachments or digital faxes as well as click hyperlinks in emails sent to them without adequate inspection are more susceptible to ransomware victimization. At the same token, department staff/officers who are more informed about the seriousness of ransomware and know indicators of potential threats in emails may be less of a target.

The presence of cybersecurity and a sufficient backup system proved to be the greatest factor for handling ransomware attacks. The NH police department case proves that saving data onto a

Table 1. Dept. Size vs. Ransom Amount.

Dept. Size (IV)	Ransom Amount
Intercept	171.12
B	76.85
p.	.009*
R square	.55

*Significance at a .05 level

backup system while having adequate cybersecurity allowed the department to avoid paying the ransom while not compromising their data due to systematic backup system. Police departments that do not have efficient cybersecurity equipped must install and have a system unattached to the main network where they can back up all of their pertinent files onto.

The findings suggest that establishing pro-social views of promoting adequate vocational activities and utilizing efficient computer security will contribute to a reduction in ransomware victimization. Therefore, acquiring adequate online lifestyle for department staff/ officers and installing computer security on the computer system have become increasingly important. Unfortunately, many police departments tend to neglect the importance of these issues.

As a micro-approach, training department staff/ police officers is essential. The training should not only address general knowledge regarding information security and valuable tips to avoid crime victimization to help prevent ransomware victimization, but also should emphasize employing adequate online lifestyles by alerting the individual to online risk-taking behavior. For example, awareness programs should focus on the management of basic cybersecurity and operations of malwares. In addition, the police departments should advise staff/officers to adopt appropriate online behaviors and avoid carelessly clicking unknown attachments in emails downloading from unfamiliar websites.

Furthermore, officers must participate in more comprehensive training in order to catch up with technology. Digital forensic training is a viable skill officers must acquire in order to makes strides in minimizing the effects of ransomware. In addition to digital forensic training, police departments should work closely with cybersecurity corporations for assistance with strengthening formal capable guardianship.

As a macro-approach, an arm control policy in cyberspace should be considered. Ransomware can be seen as an act of terror due to the danger it can produce. In Michigan, a municipal utility company was shut down for a period time due to ransomware [19]. Combine this cyber-attack with an attack in the physical realm and the damage could be catastrophic. In 2007 in Estonia, a nation dependent upon their Information and Communication technologies, suffered a major cyber-attack. Both the public and private sectors were the target of the cyber-attack, where the websites of public institutions and public e-sectors were assaulted. DDoS attacks ensued, websites were defaced, and the use of large botnets and professional coordination was present. At the peak of the attack 58 websites were shutdown, creating havoc for the country [6]. Cybercriminals in the future can easily combine ransomware with a DDoS attack, which could essentially shut down a nation's entire infrastructure, and in return get payment from their target. International cooperation is essential in order for a full suppression on ransomware and other damaging cyber-attacks.

Finally, it is important to consider proactive attempts to reduce computer/cybercrime within communities. Reducing violent cyber-attacks is an important task, yet 'reducing' cybercrime through the deployment of the suggested trainings and policies can be counterproductive in the long term. Hence, future research to produce more effective preventive measures against ransomware/malware attacks should reflect the more detailed assessment of cybersecurity and online behaviors, and the various conditions of victimization, based on individual, business, and government level.

References

[1]. O'Gorman G, McDonald G. Ransomware: A Growing Menace, Symantec Security Response.

[2]. Kaspersky Lab, Ransomware - Definition, Prevention and Removal.

[3]. (2014) U.S. Leads Multi-National Action Against "Gameover Zeus" Botnet and "Cryptolocker" Ransomware, Charges Botnet Administrator, U.S Department of Justice.

[4]. Glenn Yorkdale (2015) Criminals Continue to Defraud and Extort Funds from Victims Using CryptoWall Ransomware Schemes, Federal Bureau of Investigation.

[5]. Hill M (2016) Number of ransomware domains grew 3500% in Q1 2016, Info Security.

[6]. Choi K (2015) Cybercriminology and digital investigation. (1stedn), LFB Scholarly Publishing LLC, El Paso.

[7]. Kavid Singh (2015) The New Wild West: Preventing Money Laundering in the Bitcoin Network, Nw J Tech & Intell Prop 13(1): 37.

[8]. Murdock J (2016) US: Hackers hold Melrose Police Station to ransom for the paltry sum of one bitcoin, International Business Times.

[9]. Bray H (2015) when hackers cripple data, police departments pay ransom: Tewksbury, other departments powerless against computer hackers, Boston Globe.

[10]. Cohen L, Felson, M (1979) Social change and crime rate trends: a routine activity approach. American Sociological Review 44: 588-608.

[11]. Fitzpatrick D, Griffin D (2016) Cyber-extortion losses skyrocket, CNN Money.

[12]. Choi K (2008) Computer crime victimization and integrated theory: an empirical assessment. International Journal of Cyber Criminology 2(1): 308-333.

[13]. Danielson T (2015) The FBI says you may need to pay up if hackers infect your computer with ransomware, Business Insider.

[14]. Ngo T, Paternoster R (2011) Cybercrime victimization: an examination of individual and situational level factors. International Journal of Cyber Criminology 5(1): 773-793.

[15]. Symantec Security Response (2016) KeRanger: First Mac OS X ransomware emerges compromised BitTorrent installer used to spread ransomware that encrypts files on Mac OS X computers.

[16]. Eyal Estrin (2016) McAfee Labs Threat Advisory, Ransomware-Petya, McAfee.

[17]. Francescani C (2016) Ransomware Hackers Blackmail U.S. Police Departments, NBC News.

[18]. Newcombe T (2016) Hackers Hold Police Files Hostage for Ransom, Governing.

[19]. Smith M (2016) Ransomware attack forces Michigan utility to shut down systems, phone lines, email, Network World.