Cyber Crime Task Force Plan for St. Louis County, Missouri

Student's name

Course name and number

Instructor's name

Date submitted

I. Executive Summary

Certainly, incidences of cybercrime have tremendously increased across the world, which compromise the security of data across computer networks. As such, acts of cybercrime have reinvigorated due to the massive adoption of computer networks so immense and subtle efforts are necessary to fight them at any costs. The increased number cybercrime incidences reported to the police department at St. Louis County prove that St. Louis County is also not insusceptible to threats posed by these crimes to children, economy, public security, and privacy of sensitive information. Due to the severity of threats posed by cybercrimes in this region, the police department is committed to establishing a cybercrime task force. Hence, the proposed plan identifies the most significant cybercrime threats in St. Louis County, establishes the structure of the proposed cybercrime task force, proposes the appropriate technologies and equipment to be utilized by the task force to probe incidences of cybercrime, and establishes legislation and provisions necessary to foster the capacity of law enforcement agencies to investigate cybercrimes.

II. Threats Posed by Cyber Crime in St. Louis County

Just like other counties in the U.S., St. Louis County has heavily invested in the latest technology to reinvigorate and foster its economy. Among the latest technologies adopted across St. Louis County are computers, computer networks, and internet services. Regretfully, these technologies have been sources of threats, particularly cybercrime threats. The incidences of cybercrime reported to the police department at St. Louis County indicate that threats posed by cybercrime manifest in different forms, which vary in severity inflicted to the target victims. Some cybercrime incidences threaten public security, financial loss, and children's social health

while others threaten the privacy of sensitive or confidential information such as credit cards information and online banking passwords (Moore & IGI Global, 2017).

Cyber Crime is a major problem in St Louis as its growth is propagated in a world that is rapidly advancing in terms of technology. As the world focuses on technology, St. Louis has not been spared when it comes to the crime. Cybercrime is relatively new in the world but adopts various traits that are synonymous with other crimes. In this manner, there are many types of cybercrimes, differing in form and severity. St. Louis has experienced an upsurge in cybercrimes with advanced forms being used by different parties. While computer and net crimes are common in St. Louis, they have a varying degree of influence in the county as well as in its vicinity (Geers, 2011). For instance, some internal St. Louis net-crimes are threatening to the nation's financial health and security. Some of the cybercrime issues elicited in St. Louis have been regarded as high-profile crimes in which most deal with credit card fraud and the threat of information privacy.

Cybercrimes are observable in St. Louis in both internal and cross border form. They include issues such as espionage, financial theft, and threats to national financial health and national security (Geers, 2011). Furthermore, various types of crime adversely affect social health. These issues pertain to the family and concentrate on children and the minority in a society. They include child pornography and also child grooming, where both crimes are considered by St. Louis as high-profile (Geers, 2011). Individuals in St. Louis also experience frequent identity thefts as well as online frauds, making cybercrime have a lasting presence in the locality. Therefore, St. Louis evidences many forms of cybercrimes, providing a common ground for activities such as internet scams, phishing, password trafficking, harassment, various forms of

internet fraud, and bomb threats. Additionally, there are more common crimes in the area that are geared against minors. These include sexual predation operations and child exploitation.

The majority of cybercrimes in St. Louis are focused on individuals. However, many surveys in the area indicate that cybercriminals operate within the Missouri area, both within and outside St. Louis. In 2011, a college search in the US illustrated that about 73% of Americans have faced an aspect of cybercrime (Johnson, 2015). The figure is also high globally, standing at 65%, where 66% of many of the world's hackers are regarded as Americans (Johnson, 2015). In this manner, St. Louis is located in an area prone to cybercrime. It is also integrated within a system with the greatest number of hackers as well as the largest percentage of people who have experienced a cyber-hacking. America provides a good target for hackers, where the nation's sizeable number of enemies continue to impede cybersecurity operations while offering enemy hackers a platform to attack the US.

The High Technology Crime Investigation Association released a report detailing high-tech crimes. In this report, the researchers evidenced a 65% increase in fraudulent activities carried out on the internet. Furthermore, identity theft rose by over 60% while offenses involving child exploitation, inclusive of child pornography, increased by about 40% (Johnson, 2015). St. Louis is a member of the High Technology Crime Investigation Association and was part of the group that produced the report accounting for behavior that occurred from 2005 to 2010 (Johnson, 2015). While other forms of cybercrime existed in the area, they trailed behind the aforementioned ones. As such, general frauds conducted over the internet including identity theft, credit card fraud, and child pornography are the major contemporary forms of Cybercrime in St. Louis. Moreover, as each issue has progressed rapidly in the region, they may also indicate the area's future worst threats.

III. Cyber Task Force Structure

Cyber Crime is the most advanced form of criminal activity in the world. From the crime's development to its execution, cybercrimes are operated by smart people who operate undercover by camouflaging their network systems. Additionally, as a reflex to intensifying security alerts concerning cybercrime, these individuals have become better at dodging traps set by task forces as well as hibernating when they deem it intense to carry out their operations. Cybercrime tasks forces face numerous challenges identifying and dealing with cyber threats as they could come from any country. The internet connects the entire world, making it difficult to pinpoint a culprit's location, particularly owing to the limited interaction offered between individuals and the internet (Touhill & Touhill, 2014). Remailer services make it increasingly difficult to determine a suspect's location, further allowing cybercriminals to remain hidden.

Due to the interrelated nature of the internet, the task force involved in combating cybercrime will have to borrow its structure from preexisting tasks forces dealing with the same issue. In the recent past, researchers such as those from Finjan and investigators have developed structures to explain the cybercriminals' activities (Touhill & Touhill, 2014). While hackers have employed a mafia-like structure, the task force seeks to integrate a pyramid fused with the mafia-like structure. A pyramid structure is important when dealing with every aspect of the task force. As earlier stated, the information sought from other task forces would be used in developing better cybersecurity. Furthermore, a multi-tiered system would help to solidify the case for stronger cybersecurity. The management should adopt a mafia-like form, as used by hackers to develop a fluid management system (Touhill & Touhill, 2014). In this instance, the system is helpful to track changes in tactics, determine preference points, preference rates well as other information deemed important by the management. By merging task force designs with newly

developed cybersecurity identifiers for cybercriminal behavior, the task force will have all-inclusive cybersecurity that addresses issues evidenced by other task forces. Moreover, its ability to gain knowledge from other task forces allows the St. Louis team to continually adapt to cyber crime's changes. As the internet evolves rapidly, it is equally important for cybersecurity to grow as it is the only link between safety and exposure of sensitive information in the information age.

Personnel and Skills Required.

Different people in varying fields of operations are required to operate in the myriad of cybercrime cases that are evidenced. In this manner, issues such as child pornography and exploitation would be solved in a single department. However, sexual predation would be dealt with by different people when compared with another cybercrime, general fraud (Touhill & Touhill, 2014). Individuals involved in credit card problems differ from those who deal with children. Therefore, it is important to allocate individuals to varying cases, to maximize the results elicited. As cyber criminals vary, especially those related to cases involving minors, it is important to develop an effective cybersecurity team that is specialized in different fields. For instance, it is important to get personnel in fields such as computer forensics, intelligence as well as government and non-governmental organizations. Fluid management is the task force's key benefit, where it possesses unique and differentiated skills beneficial to provide security. As such, while specialists in computers would develop better technology, individuals in the cybersecurity field are constantly looking for ways to improve their intelligence. Finally, accounting personnel are important to determine the likelihood of credit card fraud as well as other cases related to internet fraud.

Task Force Collaborations

The task force requires to build strong and effective connections with other federal agencies as well as with other bodies within and outside St. Louis County to be effective. Many federal bodies such as the Federal Bureau of Investigations (FBI) and the National Security Agency (NSA) have existed for a long time. As a result, they have developed highly-sophisticated methods of hacking, frequently employing their knowledge and expertise to avoid national and regional calamities. Similarly, the task force is developed to prevent various criminal activities such as child pornography from proliferating in Missouri. In this manner, it is prudent to seek information from federal bodies such as the FBI and the NSA to gain accurate information on a subject. Federal agencies have been operational for longer than the task force, where they can better understand demographic dynamics as well the area where they operate.

The task force will create a relationship with Safe Streets, a task force developed to unify local, state, and federal agencies in a bid to fight criminal activities. The Cyber Crime Task Force would also be a good addition for the task force's collaborative team as it has been fighting cybercrimes for some years. Moreover, the St. Louis Terrorism Task Force will be sought after as a partner, where its efforts to unify the 40 local, state and federal agencies has led to a better investigation of terrorism leads, boosted support in special events and enabled nations to determine potentially dangerous areas for cybercriminals (Geers, 2011). The task force would also work with the Internet Crime Against Children (ICAC), a task force aimed at preventing children from being harassed using technology. The task force will also work in collaboration with other groups such as the St. Louis InfraGard Chapter (Geers, 2011).

IV. Task Force Equipment

Types of Equipment Required.

The Cybercrime task force requires several types of equipment, technologies, as well as other items to function optimally. For instance, a well-equipped laboratory for computer forensics and other field equipment discussed here below would form a large part of the task force's operations (Kamberg, 2018).

Necessities to Build a Forensics Cyber Crime Lab

Firstly, the forensics lab equipment to be used includes evidence packaging, a first responder tool kit, remote chargers, portable forensic towers, wireless stronghold bags, mobile tracking devices, and write protection forensic devices (Kamberg, 2018). Moreover, forensic scientists will need various software tools for optimal operations. These include DIBS Mobile Forensic Workstation, CelleBrite UFED Systems, and DeepSpar (Kamberg, 2018). It is also important to use tools such as LiveDiscover, CD/DVD inspector, Logicube, Image MASSter, and InfinaDyne Forensic Products (Kamberg, 2018). Additionally, tools such as TEEL Technologies SIM Tools are necessary for effective cybersecurity and thus good for the task force. One should also consider the importance of technologies and other items such as printing papers, magnifying glasses, small flashlights, seizure disks, large rubber bands, and gloves.

Furthermore, the task force will use these techniques to determine the results of items in its forensic investigations. To begin with, it will employ cross-drive analysis for investigating and detecting anomalies as well as social networks (Kamberg, 2018). The forensic process also dictates that individuals in the task force use live analysis for computer inspections. A live analysis is helpful for computer inspections conducted within an operating system using either forensic tools or sysadmin techniques where evidence extraction is deemed paramount (Kamberg, 2018). It is also important to consider that any future techniques integrated into

cybersecurity will be used by the task force as it determines that technology is a dynamic truth. As such, cybersecurity has to stay ahead of its malicious counterparts to alleviate cybercrime.

Importance of these Systems

A cybersecurity system is an important component of any task force. It is important as its hardware and software components are widely deemed as relevant in Forensics labs. As such, a cybersecurity system is necessary as it forms the avenue for executing cybercrime investigations.

V. Cyber Crime Legislation

Legislation and Provisions to boost Local Law Enforcement Capacity to Investigate Cyber Crime

Legislations and provisions are necessary for St. Louis County to pursue cybercriminals as they would boost the capacity of local law enforcement to conduct cybercrime investigations. For instance, the judges appointed to law courts in St. Louis should be cyber-savvy, whereas proactive laws implemented within the county should also seek to enforce cybercrime policies. Furthermore, it would be prudent to ease internet laws across various jurisdictions such as states as it would lead to a unified combating effort for internet crimes (Moore & IGI Global, 2017). While child pornography and sexual predators continue to exhibit increased scrutiny and review, the loopholes evidenced in the system are minimized. Specifically, legislation that reinforces the Protect Our Children Act of 2008 would help to curtail child exploitation (Larence, 2011). It is prudent to boost local, state and federal agencies' capacities as they should be able to deal with high-tech criminals such as cybercriminals. Provisions such as relaxed laws on police cyber monitoring should be enacted to provide law enforcement with the capacity to seek out hackers.

Where the Laws should be enacted.

Firstly, the state of Missouri should pass legislation to enact cybersecurity while shunning cybercrime. State action would be helpful as it would provide residents with information about potential hacks as well as ways to mitigate these hacks. Moreover, it is important for state laws to be developed, emphasizing on penalties to be incurred if an individual has conducted a cybercrime. Many states do not have widespread repercussions for cybercriminals, where small penalties do not mitigate criminal activity. Therefore, a widespread ban on cybercrime, as well as severe punishments would alleviate the level of cybercrime in St. Louis.

Furthermore, while a state can enact serious cybersecurity laws, they would be impeded if the federal government did not take the issue seriously. Differences in the levels of law enactors play a role in the development of cybersecurity within a state (Moore & IGI Global, 2017). Federal laws allow cybersecurity agencies to flourish as they can operate across jurisdictions.

VI. Conclusion

Cybercrimes involving general fraud conducted over the internet, identity fraud, and child pornography that are elicited in St. Louis can be dealt with using a special police task force. Task forces lay a major role in mitigating cybercrime, a rapidly rising form of criminal activity that takes place across the world.

Cybersecurity involves educating the public on issues that are pertinent to the internet. It also illustrates that vulnerable nature of users, as well as how they interact with a computer's graphical user interface (GUI) to elicit results. In this manner, educating the public on the forms

of cybercrime, as well as how to avoid being hacked would go a long way in stopping rapid cyber-attacks as is common in contemporary society.

In conclusion, cybercrime is a relatively new phenomenon in the world. However, its rapid integration in contemporary crime makes it necessary to defend against for future safety. As the criminal world becomes digitized, criminal fighting units of the police should be set up to disrupt their digital activities. As such, cybercrime would be combated in real-time, alleviating the potential for new and devastating cyberattacks to be launched without adequate countermeasures being put in place to disrupt their operations.

References

Geers, K. (2011). *Strategic cyber security*. Tallinn, Estonia: CCD COE Publication.

Johnson, T. A. (2015). Cyber-security: Protecting critical infrastructures from cyber attack and cyber warfare. Boca Raton : CRC Press/Taylor & Francis Group.

Kamberg, M.-L. (2018). Cybersecurity: Protecting your identity and data. New York : Rosen Central.

Larence, E.R. (2011). *Combating Child Pornography: Steps Are Needed to Ensure That Tips to Law Enforcement are Useful and Forensic Examinations are Cost Effective*. Collingdale: Diane Publishing.

Moore, M., & IGI Global,. (2017). Cybersecurity breaches and issues surrounding online threat protection. Hershey, Pennsylvania (701 E. Chocolate Avenue, Hershey, PA 17033, USA) : IGI Global.

Touhill, G. J., & Touhill, C. J. (2014). *Cybersecurity for executives: A practical guide*. Hoboken, New Jersey: John Wiley & Sons, Inc.