Journal of Forensic Sciences And Criminal Investigation
ISSN: 2476-1311

Juniper Publishers key to the Researchers

Review Article
Volume 18 Issue 5 - October 2024
DOI: 10.19080/JFSCI.2024.18.555998

J Forensic Sci & Criminal Inves

An Update on Cybercrime Enforcement at Localities

Richard S Groover*

Environmental Science & Public Policy, George Mason University, United States

Submission: September 16, 2024; **Published:** October 17, 2024

***Corresponding author:** Richard S. Groover, PhD, Environmental Science & Public Policy, George Mason University, United States, Email: rgroover33@gmail.com

Keywords: Computer-related Crime; Forensic investigators; Criminals

Introduction

In 1996, a Point of View article titled Overcoming Obstacles: Preparing for Computer-related Crime was published in the FBI Law Enforcement Bulletin [1]. The concern was that local law enforcement agencies, police and sheriff departments, were not prepared for future criminal acts that would involve computer technology. Some of the issues included: problems finding individuals in law enforcement with the technical expertise as well as investigative training to deal with computer crime, the absence of proper training for their staff, the vast amounts of new software coming on the market, and the variety of other issues related to the emerging technical science of computers. An additional it was reported was "In the past fewer than 10% of criminals possessed computer skills (in 1996); but by the year 2000 nearly 90% will be computer literate [1]." So, it is now 2024, and where do these issues stand, especially for law enforcement agencies?

Progress By 2017

As covered in a posted article by David Griffith on the Police Law Enforcement Solutions website [2] much progress in this area has occurred. The Police Executive Research Forum (2013) helped define what cybercrime was. Griffith also reported that the Federal Bureau of Investigations had set up the Internet Crime Complaint Center. Additional reported that The Secret Service Federal Agency had organized 37 Electronic Crimes Task Forces in the United States and two overseas in London and Rome. The FBI, to assist local agencies, were operating 15 Regional Computer Forensic Laboratories to assist with digital data analysis by 2017. But Griffith stated that much more needed to be done.

The Federal Bureau of Investigation

The FBI has published a report on some cybercrime in the United States: Internet Crime Report 2023. Most of what is covered in their report are reported data across the United States.

i. **The report states:** Today's cyber landscape is threatened by a multitude of malicious actors who have the tools to conduct large-scale fraud schemes, hold our money and data for ransom, and endanger our national security. Profit-driven cybercriminals and nation-state adversaries alike have the capability to paralyze entire school systems, police departments, healthcare facilities, and individual private sector entities.

ii. **Additionally, Their Report States:** In 2023, IC3 [the FBI Cyber Crime unit] received a record number of complaints from the American public: 880,418 complaints were registered, with potential losses exceeding $12.5 billion. This is a nearly 10% increase in complaints received, and it represents a 22% increase in losses suffered, compared to 2022. As impressive as these figures appear, we know they are conservative regarding cybercrime in 2023. Consider that when the FBI recently infiltrated the Hive ransomware group's infrastructure, we found that only about 20% of Hive's victims reported to law enforcement. More reporting from victims would mean superior insight for the FBI [3].

One Local Agency

The Hanover County, Virginia, Sheriff's Office is a full-service department, north of Richmond and handles law enforcement

for a 473 square mile county. For the last several years, under the leadership of the Sheriff, Col. David Hines, this agency has advanced and might be recognized near the top as a mid-range law enforcement agency. This department has approximately 300 employees, including patrol deputies, investigators, court services and staff. What Hines created was a very well equipped and trained Digital Forensic Unit. They have numerous computer systems operated by a small staff (3 people) of forensic investigators. This was not inexpensive or quick to achieve, as it took years and money to accomplish. This agency spent over $200,000 to set up the monitor and investigation computers in a secure room, which included the necessary software. Special training of each investigator took about $60,000 and it took nearly three years for the investigators to be fully certified [4].

For a law enforcement investigator to be fully trained and the agency to be fully equipped for the best criminal investigation and prosecution, this is the list of what Hanover's forensic investigators have:

i. LexisNexis TraX Subject Matter Expert in Call Detail and Geolocation Record Analysis

ii. Cellebrite Certified Operator (CCO)

iii. Cellebrite Certified Physical Analyst (CCPA)

iv. Cellebrite Certified Premium Operator (CCPO)

v. Magnet Forensics: Magnet Certified Forensics Examiner (MCFE)

vi. International Association of Computer Investigative Specialists (IACIS): Certified Forensic Computer Examiner (CFCE)

vii. OpenText: EnCase Certified Examiner (ENCE)

viii. Magnet Certified Graykey Examiner (MCGE)

ix. Axon Investigator Operator and Examiner

Law enforcement agencies maintain hardware (cell phones, computers, etc.) stored as physical evidence, there is also the necessary downloaded data storage needed for quick retrieval and prosecution. Hanover County Sheriff's Office is currently computer storing 250 terabytes of data from their investigations and prosecutions [4].

Training & Technical Support Available

There is an organization that provides cybercrime services for agencies. The National White Collar Crime Center in Richmond Virginia is available. Their contact for available training and technical support is: https://www.nw3c.org/UI/Index.html. About 70% of their training is for state, local, and tribal law enforcement departments, and they have trained personnel at over 18,000 agencies (Cohen 2024). Their technical support clients are 98% state and local agencies. If more formal academic training is sought, four universities provide course work and degrees. They are George Mason University, Michigan State University, California State University and the University of San Francico. George Mason has several college credit undergraduate and graduate courses to consider: CRIME 490, 595, and 795, all are cyber-crime topical courses [5].

Responsibility of the Citizens

Law enforcement cannot do it all. If a citizen has a computer or even a cell phone that has computer with mini-computer technology, it is important for that citizen to be aware and vigilant against computer attacks via emails, suspicious offers, malware attempts, etc. Training regarding such is available.

Summation

As statement of changing reality for law enforcement, in an interview with a former bank robber, he stated:

If I rob a bank, I might only get $5,000, and I might get shot by a cop and if caught it is a longer prison sentence. If I do cybercrime and can make maybe $50,000, and I probably won't get caught and the prison term is much shorter [6]. Cybercrime investigation and prosecution is very expensive. Considering equipment, software, and investigation training many state police are spending $6 million a year [6]. Expensive but critical in today's landscape. Dr. Jin R. Lee at George Mason University points out that most traditional street crime is now moving online [5]. Drugs are illegally sold via internet orders. Criminals often communicate their plans via cell phone messages, sometimes very straight forward, sometimes even coded/encrypted. The emerging technology of Artificial Intelligence may present more crime investigative challenges. Dr. Lee suggests local agencies look at two questions regarding this topic: Where is the problem … What is our best strategy for addressing this?

References

1. Groover Richard S (1996) Overcoming Obstacles: Preparing for Computer-related Crime. FBI Law Enforcement Bulletin 65(8): 8-10.
2. Griffith David (2017) Fighting Cybercrime at the Local Level. Police Law Enforcement Solutions Website.
3. Federal Bureau of Investigations (2023) Internet Crime Report 2023. United States.
4. Cary Tyler (2024) Personal Interview, United States.
5. Lee Jin R (2024) Personal Interview, United States.
6. Cohen Charles (2024) Personal interview, United States.

How to cite this article: Richard S Groover. An Update on Cybercrime Enforcement at Localities. J Forensic Sci & Criminal Inves. 2024; 18(5): 555998. DOI: 10.19080/JFSCI.2024.18.555998

DOI: 10.19080/JFSCI.2024.18.555998

How to cite this article: Richard S Groover. An Update on Cybercrime Enforcement at Localities. J Forensic Sci & Criminal Inves. 2024; 18(5): 555998. DOI: 10.19080/JFSCI.2024.18.555998