Starting a CyberCrime Unit:

Key Considerations for Police Chiefs

POLICE EXECUTIVE RESEARCH FORUM

Nearly every crime has a digital component. As such, police leaders are under increased pressure to dedicate resources to combat cyber-enabled crime. The purpose of this document is to offer law enforcement executives key considerations for establishing a cybercrime unit, including: scope, recruitment/staffing, inter-agency partnerships, training, and funding.

Key Considerations:

Scope: Cybercrimes vary in technical complexity. They range from traditional crimes that contain a cyber component (e.g., computer-*enabled* crimes such as cyberbullying), to more advanced computer crimes (e.g., hacking, swatting). When starting a cybercrime unit, agency leaders must assess the department's needs in order to establish appropriate unit capabilities and determine areas of investigative responsibility. Are you establishing your cyber unit to provide support for traditional investigations, or is the unit focused on investigating complex computer crimes? Defining the scope will guide you when determining funding, staffing, equipment, and training needs.

Recruitment: Staffing is a crucial component to building a strong cybercrime unit. When recruiting from within the department, first-line supervisors can be a valuable resource to help you identify talent in your agency. If a patrol officer has a reputation among their shift for being tech-savvy, for example, the sergeant will lead you to them. Department leaders may also consider recruiting from outside of the agency. Staffing a cybercrime unit with civilians is cost-effective and keeps police officers in law enforcement roles- a concern among many police departments facing shortages of officers.

Inter-agency Partnerships: When forming a cybercrime unit, department leaders must abandon the silo mentality and build collaborative partnerships with local, county, and state agencies. You may consider forming an ad hoc group with neighboring jurisdictions, entering into a county or state-wide task force, or establishing a formalized partnership through an MOU. Forging these relationships allows you to combine resources and facilitate information sharing at the local, state, and federal level. [1]

Training: Budgetary constraints are often a significant hurdle for securing quality training for cybercrime personnel. Fortunately, there are many sources of free or low-cost training offered to cybercrime investigators.

- **National White Collar Crime Center (NW3C)** provides online and in classroom training for conducting cyber investigations and processing digital evidence. NW3C also offers a Cyber Crime Examiner Certification.[2]

- **Federal Virtual Training Environment (FedVTE)** offers free online cybersecurity training on topics such as cybersecurity investigations and mobile forensics. [3]

- **National Computer Forensics Institute (NCFI)**, supported by the U.S. Secret Service, offers basic and advanced examiner courses for cyber investigators. Training fees, travel expenses, lodging, and equipment are provided at no cost to the attendee or their department.[4]

- The **Cyber Investigation Certification Program (CICP)** is a course offered by the FBI that is designed to teach police officers how to secure a crime scene with a digital component and preserve digital artifacts. The training is available through Law Enforcement Enterprise Portal (LEEP).[5]

Additional training opportunities can be found through the Law Enforcement Cyber Center's Training and Conference Search Tool. This resource allows users to search for upcoming online and in-person training classes, conferences, and other events in a single database.[6]

Funding: Funding is a concern for many police leaders interested in starting a cybercrime unit. Fiscal restraints, however, should not deter departments from investing in cyber investigations. There are three primary monetary sources to fund your cybercrime unit.

- **Operating budget**: A department's priorities are often reflected in an operating budget. As such, department leaders must make the case to their community and city council members that investing in cyber investigations is essential for public safety purposes. Allocating funds in the operating budget is crucial for sustaining a cybercrime unit.

- **Grant funds**: Grant funds may be available to assist you in funding your cyber crime unit. If you are unsure of where to start, policegrantshelp.com features a grant database that allows the user to search for local, state, federal, and corporate grant opportunities.

- **Forfeiture funds**: Police chiefs may consider using seized funds to invest in their cybercrime unit.

Conclusion

The proliferation of technology has caused an influx of digital evidence and cyber-related crimes that police departments must be prepared to address. Starting a cybercrime unit can be a daunting task for any police executive, but one that cannot be ignored. With these key considerations in mind, police leaders are better equipped to establish a cybercrime unit and combat cybercrime in their jurisdictions.

---

[1] An example of an inter-agency partnership is demonstrated by the New Jersey Regional Computer Forensics Laboratory (RCFL). The RCFL comprises representatives from federal, state, and local entities that provide digital forensic services to New Jersey law enforcement agencies. For more information, see https://www.rcfl.gov/new-jersey

[2] See https://www.nw3c.org/

[3] See https://fedvte.usalearning.gov/

[4] See https://www.ncfi.usss.gov/ncfi/

[5] See https://fbi-cicp.cert.org/lms/

[6] See http://www.iacpcybercenter.org/training-and-conferences/