CYBERCRIME: WHAT CAN A GOVERNOR DO?

The state and local officials that comprise the homeland security and public safety community must confront all hazards to the public, including cybercrime. Yet many of those charged with investigating and prosecuting cyber criminals lack the technical expertise, resources, and overall capacity to do so. Because of such limitations, state and local agencies typically can only address the smallest incidents on a piecemeal basis. And solely relying on federal criminal investigators is not a sustainable solution, as they typically investigate only the most serious cybercrimes. That leaves a large set of victims without recourse. On December 11, 2018, the National Governors Association (NGA) convened over two dozen experts on cybercrime to explore how states can build capacity for cybercrime enforcement at the state and local levels.

Ongoing Challenges to Building Capacity for Cybercrime Enforcement

Cybercrime enforcement is new

State and local cybercrime enforcement is still an emerging field as cyber attacks continue to grow in scope, complexity, and severity, and many state cybercrime units are experiencing growing pains. For example, integrating digital investigative techniques with traditional methods—a necessary process if investigators want to trace cybercrimes to suspects in the real world—remains a challenge in many jurisdictions.

Cyber criminals are elusive

Many cyber criminals operate across jurisdictions, and perpetrators and victims may be separated by thousands of miles and international borders. Notwithstanding any technical challenges related to identifying a perpetrator, indictment and prosecution often requires tackling a series of legal and political obstacles. Even where these challenges do not kill investigations outright, they can discourage state and local law enforcement from pursuing leads.

Turnover and loss of knowledge

Turnover is a serious challenge because experienced investigators often leave for the private sector, where salaries greatly exceed those offered by law enforcement agencies. Exacerbating the situation is a lack of promotional opportunities within high-tech units, encouraging those who want to advance to transfer to other units where they can advance their career.

Institutional resistance

Some stakeholders raised concerns that because traditional demands on law enforcement are not going anywhere, adding a new, resource-intensive responsibility may not be feasible. Investing in cybercrime enforcement may drain resources from more traditional functions, such as combating homicides, upgrading patrol equipment, or strengthening community engagement. Striking the right balance can be a challenge.

Lack of basic training and specialized personnel

Many law enforcement agencies do not require in-depth training for law enforcement officials on basic cybercrime concepts, such as recognizing and preserving digital evidence or basic prevention techniques. Specialized training for cybercrime investigators or digital forensic examiners is costly, time-consuming, and may be challenging to find on a local or regional basis. Due to its technical nature, law enforcement agencies note that it can take an extensive amount of time to become proficient in cybercrime investigations relative to other more traditional investigations. Trained personnel are frequently overwhelmed by an endless backlog of requests to examine digital evidence or respond to cybercrime complaints.

Recommended Steps for Governors

Create a cybercrime strategy

As a first step, governors should develop a formal strategy to strengthen cybercrime enforcement. An effective strategy seeks to coordinate initiatives, encourage resource-sharing, and align priorities across agencies. It should include or accompany a detailed implementation plan (perhaps in an executive order) assigning roles and responsibilities, with clear deadlines for agency actions. Importantly, a strategy should clearly articulate how to measure progress. Feedback should be solicited from a wide range of stakeholders during the drafting process

Use the cybercrime strategy to advocate for more resources

Many best practices in cybercrime capacity-building will require additional funding. Governors should work with law enforcement agencies to identify potential champions in the legislature and use the cybercrime strategy to demonstrate to legislators that additional appropriations will be spent in a thoughtful manner. Governors should also enlist help from the businesses community and citizens who have been victims of cybercrime, asking them to provide input on the real-world impact of cybercrime.

Revise laws that undermine cybercrime enforcement

Governors should rely on their cybersecurity governance entity or collaborate with your attorney general to work with legislators, investigators, public attorneys, judicial officers, and other relevant stakeholders to identify how state law impedes cybercrime investigations, and craft legislation to amend the law accordingly. Substantive changes may include modifying the standard of intent for computer trespass or revising associated penalties. States might also want to revisit criminal procedure, e.g., rules that govern the investigative process or the verification of electronic evidence.

Institutionalize knowledge requirements

Governors can determine who sets the standards that police officers must meet (in many states it is a commission), and work with appropriate authorities to ensure standards include proficiency in relevant competencies. Police academies could introduce cybercrime and digital evidence concepts to all officers, working with federal partners, the private sector, and qualified volunteers to supply instructors. Police academies could then establish a process for identifying especially capable cadets who would benefit from additional specialized training not offered by state government. However, any new training standards should align with a cybercrime strategy outlining who should be trained, when, and for what purpose.

Reduce the victim population by increasing education

Many cybercrimes can be avoided through simple security measures that all computer users can practice. Law enforcement agencies already educate the public with information sessions on methods to deter traditional crime. Any outreach efforts—whether they are town halls, pamphlets, or news interviews—should include information on good cyber hygiene for individuals and businesses. Law enforcement should never miss a chance to hammer home the basics. Simply reducing the incidence of cybercrime will allow state and local law enforcement to concentrate limited resources on the most serious cases. Alternatively, a consolidated statewide cybersecurity office might take the lead on public education with the support of law enforcement.

Encourage external engagement

A series of federal, private, and non-profit organizations offer cybercrime training opportunities and technical assistance to state and local personnel. Many of these bodies already collaborate through regional task forces, which can be leveraged for capacity and resources by state and local agencies. Governors should also ensure that police departments have a dialogue with these task forces and with local and regional federal investigators and prosecutors. Governors could also charge their cybersecurity governance entity with educating state and local police agencies on available opportunities and partners, such as the Internet Crimes Complaint Center (IC3). Lastly, governors can encourage them to request assistance from relevant national-level associations, including the National Governors Association, and to apply for grant funds for external training and capacity-building.

Institutionalize continuous cyber-crime training for state and local law enforcement

Cyber-crime training should continue throughout an officer's career. Organizations like the National White Collar Crime Center (NWC3) and multiple federal entities—such as the U.S. Secret Service's National Computer Forensic Institute—offer trainings for officers at all levels. Governors should consider using the same training program for multiple agencies (state and local). Educational opportunities for executives and mid-managers are especially important, instilling realistic expectations and establishing mid-level commitment to cybercrime initiatives. Law enforcement agencies should explore whether and how trainings or other education can be provided to judicial clerks as well. These officials may not have relevant cybercrime expertise nor knowledge and would therefore need cyber-crime training to try a case successfully.

Collaborate with local colleges and universities

Governors' offices should work with higher education institutions to develop a "cybercrime curriculum" for pre-law students, criminal justice majors, and other relevant majors to ensure that recruits, prosecutors, clerks, and judges have at least some familiarity with cybercrime tactics and investigative methods. Governors' offices should encourage universities to establish internship programs to introduce students to the new, technology-oriented opportunities that are available in law enforcement. Lastly, universities should collaborate to create or enhance reimbursement programs for current law enforcement officers to receive similar education. Governors should ensure that law enforcement leaders meet regularly with cybersecurity experts in academia and the private sector, and explore an anonymous communications channel that will allow these outside experts to provide tips to police.

For questions and comments, please contact David Forscey at dforscey@nga.org or Michael Garcia at mgarcia@nga.org.