MEET the THREAT

States Confront the Cyber Challenge

Cybersecurity and Public Safety
October 25th, 2016

Cybersecurity is a Core Concern for the Public Safety Community

The state and local officials that compose the homeland security and public safety communities must confront all hazards to the public, including those caused by cyber attacks. Their collective role in cybersecurity has three dimensions, each presenting its own challenges. First, criminal investigators and prosecutors are charged with tracking computer crime and convicting perpetrators. Unfortunately, many local jurisdictions lack the proper technical expertise to do so. Second, homeland security advisors, law enforcement officials, and first responders must grapple with real-world effects of significant cyber incidents. Yet in many communities, these stakeholders have not formulated procedures to coordinate a response to cyber emergencies. Third, state agencies and local first responders must protect their own computer systems; they cannot fulfill their duties without communications or access to mission data. A long list of attacks on these entities demonstrate that many remain unprepared to protect critical systems, let alone chase computer criminals or coordinate a response to a destructive cyber attack.

Ongoing Challenges to Improving Public Safety Involvement

Inconsistent focus on cybersecurity: Many public safety agencies and first responders do not include cybersecurity as an indispensable element of operations, planning, and procurement decisions.

Confused roles and responsibilities: States often lack a strategic framework for managing the role of public safety personnel in cybersecurity planning and response. For example, many public safety officials do not have contacts at national response centers.

Cultural resistance: Some might resist expanding the function of public safety personnel to include cybersecurity, arguing that resources should be devoted to more traditional roles. Many homeland security professionals want to focus on counter-terrorism, which tends to involve detecting and preparing for physical violence.

Recommended Steps for Governors

Public safety outreach: Convene state and local leaders in homeland security and public safety to assess current capabilities, ongoing efforts, existing gaps, and future needs in cyber threat mitigation.

Develop a comprehensive strategy: Governors should direct stakeholders to draft a statewide cybersecurity strategy that articulates clear roles for homeland security stakeholders, public safety agencies, and the National Guard.

Use exercises to identify vulnerabilities and solutions early: Exercises help law enforcement and emergency personnel evaluate current protocols and procedures and examine whether modifications are necessary. Major exercises also offer a public demonstration of the possible physical consequences of a major cyber incident, serving to educate citizens and legislators who might overlook the threat.

Capitalize on existing assets, plans, and principles: Since 2001, the homeland security and public safety enterprise has worked hard to implement time-tested risk management practices. These principles and the resulting infrastructure can be adapted to account for cyber threats. For example, many states have established fusion centers designed to detect and prevent terrorism, and they may be ideally positioned to share cybersecurity threat intelligence across state and local government and with private sector partners. Similarly, many homeland security offices have instituted the proper frameworks—often compatible with federal assistance principles—to coordinate an effective response to cyber attacks. With minor modifications to existing plans, states can save the time and energy needed to draw up entirely new response frameworks.

Encourage personnel exchanges between agencies: Intelligence agencies long ago institutionalized the practice of swapping personnel to improve collaboration and develop well-rounded expertise throughout their workforce. Governors should encourage similar partnerships between departments that focus on cybersecurity and public safety agencies. Such arrangements would help build the personal and institutional relationships that are the foundation of a whole-of-government approach to cybersecurity and incident response.

Deploy resilient emergency communications: A disabling attack on IP-based communications could prevent emergency personnel from communicating. Agencies should ensure they have back-up analogue systems, and that all personnel are trained on how to use them. However, resilient communications equipment is expensive, and so Governors should utilize the substantial influence of public safety groups to win the necessary resources from state legislatures.

Boost federal assistance: States should work with federal agencies to improve policies and procedures governing cybersecurity assistance grants, encourage state agencies to apply for current assistance programs, and advocate to Congress to boost related funding.

Please e-mail Timothy Blute, Program Director, Homeland Security and Public Safety Division, NGA at: tblute@nga.org *with any questions.*