Cyber Incident Response to Public Safety Answering Points: A State's Perspective

Background

Public safety answering points (PSAPs) are increasingly being targeted by malicious actors seeking to disrupt emergency communications systems and operations. Across the country, PSAPs with varying levels of resources and response capabilities are facing complex and sophisticated cyberattacks.[1]

This case study highlights one state's response to cyber incidents involving PSAPs, including the legislation surrounding their authority, the collaboration required for a successful response, and best practices for entities preparing for cyberattacks. The Cybersecurity and Infrastructure Security Agency (CISA), SAFECOM, and National Council of Statewide Interoperability Coordinators (NCSWIC) collaborated with state public safety and emergency communications stakeholders to develop the case study and share lessons learned from responding to cyber incidents. This document provides actionable tips to help emergency communications centers (ECCs)/PSAPs prepare for and respond to cyber incidents.

Governance

To better respond to cyber incidents, the state governor signed an executive order establishing a cybersecurity integration center (CIC). Two years after the executive order was signed it became law, providing funding to expand the center's cybersecurity capabilities, including additional staff for intelligence, operations, and incident support.

The CIC is comprised of state agencies, including police, information technology (IT), emergency services, the military department, and local and federal partners, such as CISA and the Federal Bureau of Investigation (FBI). These agencies have established relationships and pre-determined responsibilities to engage in CIC-assisted cyber incident response and recovery.

Response

To address cyber threats, the state's governance document outlines processes for reporting and responding to cyber incidents. The state has IT personnel available 24 hours a day for PSAPs to report incidents and outages. When a PSAP reports an incident, it is processed using an incident report, given an escalation rating using a scale of one to five, classified by the type of incident, and then assigned to the appropriate agency or department for further assistance.

Information about the reporting PSAP, type of threat, and systems impacted are used to determine the state's response. An example timeline of a larger cyber incident response is as follows:

[1] CISA's *Transition to Next Generation 911 (NG911)* web page provides resources and best practices for ECCs/PSAPs to secure NG911 systems.

After an entity reports a cyber incident, the first phase of response is to gather information on the specifics of the attack and system attributes.

The second phase is to develop an incident-specific response plan and identify any resources needed. The response varies depending on the needs and capabilities of the reporting entity, as some larger agencies have additional resources available.

By phase three, the state response team is deployed for on-site assistance and forensic evidence collection. As a condition of the state's response, they require a representative from the PSAP to be on-site 24 hours a day to assist as needed.

State-level response can vary depending on the criticality and complexity of the incident. For more complex incidents, the on-site response is typically one to two weeks to identify and respond to the cyber threat. They may provide the PSAP with:

- On-site support
- Recommended points of contact to assist with remediation efforts
- Assistance brokering between the PSAP and their cybersecurity insurance provider, if applicable

For long-term events, the state response team supplements their staffing plan to prevent burn out. This is especially important if there are simultaneous attacks. In these cases, the state engages with partners, such as the National Guard, to assist with response operations and implements a staffing rotation plan. The state works collaboratively with partners to identify potential threats, share intelligence, and provide no-cost scans of an agency's networks.

Future Plans

The state is currently developing a case management system to capture metrics on cyberattacks to help identify trends and threats. They are also developing a cloud-based incident reporting system for entities to report incidents and submit tickets through a mobile application or by phone. Additionally, they plan to increase capacity to deploy rapid incident response teams to incident sites.

Lessons Learned

Develop strong cyber incident response and vulnerability response plans

ECCs/PSAPs should develop cyber incident response and vulnerability response plans. Cyber incident response and vulnerability response plans can provide agencies with a roadmap to follow during cyber incidents to minimize confusion. These plans should include up-to-date contact lists and detailed steps for agencies to take in the event of an incident. Staff should be trained on cyber incident response. Plans should be tested (e.g., tabletop exercises) and updated regularly.

Provide incident reporting 24 hours a day, 7 days a week, 365 days a year

Cyber incidents are not limited to normal working hours. ECCs/PSAPs should consider the need for on-call support, especially for incidents that take place after business hours, on weekends, or holidays. The ability to contact live, real-time support to walk through next steps can mitigate damage and improve response and recovery.

Establish relationships with partners prior to a cyber incident

Responding to cyber incidents involves collaboration across multiple agencies. ECCs/PSAPs should establish relationships with partners prior to an attack to help ensure a seamless response. These relationships may include service providers, neighboring agencies, and state, local, and federal agencies. Including partners in exercises, trainings, and response plan development helps ensure agencies and partners are familiar with their roles and responsibilities responding to a cyber incident.

Document network systems and architecture

ECCs/PSAPs should maintain awareness of their networks and assets, including hardware and software inventories and information regarding internal and external network connectivity. Familiarity with architecture and systems can greatly improve response effectiveness and timeliness because it reduces the time needed for responding agencies to gain knowledge about the network prior to gathering evidence and identifying and responding to a threat. It is recommended that ECCs/PSAPs know who has access to systems, ensure there is a business need, and establish user access agreements to outline user permissions and expectations. ECCs/PSAPs should proactively review vendor contracts, agreements, and data to define how data is handled, vendor infrastructure and practices the vendor utilizes, and each vendor's responsibilities in an incident.

Practice good cyber hygiene to reduce the risk of cyberattacks

ECCs/PSAPs should implement good cyber hygiene in their daily operations. ECCs/PSAPs can use resources, such as the *Public Safety Communications and Cyber Resiliency Toolkit*, to discover public safety-specific cyber guidance. ECCs/PSAPs should consider developing or refining authentication and password policies including strong, unique passwords requirements and multi-factor authentication, where possible.

Implement cyber threat detection capabilities

ECCs/PSAPs should consider implementing cyber threat detection and mitigation capabilities and using resources such as fusion centers. These state and local centers may provide system monitoring, threat identification, and intelligence sharing, allowing ECCs/PSAPs to maintain a proactive cyber posture.

For more information on this and other cybersecurity initiatives, contact ng911wg@cisa.dhs.gov or visit cisa.gov/safecom/next-generation-911 and cisa.gov/communications-resiliency.