911 Service Interruptions, TDoS, and Reporting

Harriet Miller-Brown

911 Tech Forum

April 18-19, 2017

Objective

- This presentation is meant to do two things:

1) Outline the current guide for before, during, and after a 911 outage or service interruption.

> This includes PSAP staff of all levels, local emergency management coordinators, communications network providers and technicians, command and response personnel at the Michigan State Police Operations Desk (MSP Ops Desk), and other parties who may be involved.

2) To look beyond 911 “traditional” outages and to look at other 911 system interruptions such as TDoS or other immediate cyber security threats/events impacting 911 service.

Definitions

- 911 Outage or Service Interruption:

  The loss of 911 connectivity from any point in the communications network (wireless, wireline, or IP) supporting or delivering 911 services.

- Partial 911 outage:

  A loss of 911 service within a limited geographical area, within a PSAP service area, or a loss of service with only a specific provider (i.e. a single VoIP or wireless service).

- Non-emergency phone service outage:

  Loss of service to PSAP non-emergency lines and numbers.

- Telephony Denial of Service (TDoS):

  An interruption in a PSAP's ability to answer incoming 911 calls; where a perpetrator uses the telecommunications system to create a flood of calls into the PSAP through the use of auto-dialing machines or by other means of network disruption.

What to do?

- Internal policies and protocols should be in place in advance!
- The policies should be based on the individual PSAP's communication capabilities.
- Policies should be accessible to all and updated. Some considerations:
  - Will all 911 calls need to be transferred to another PSAP?
  - Will the public need to be provided any specific instructions?
  - Will additional staffing be needed?
  - Will staff need to be sent to another PSAP?
- Notifying or manning back-up PSAPs.
- Contacting PSAP management.
- Alerting local public safety responders.
- Notice to the public.
- Activating media/social media and other alerting systems
- Creating a press release including public instruction

PSAP-initiated notices of outage or interruption

- Circumstances may exist where the PSAP knows there is an issue before a communications provider does:
  - Make contact with the appropriate 911 Resolution Center immediately.
  - If communication outside of the PSAP is lost through phones and radio, other sources may prove effective:

    1) LEIN system

    2) The MSP Ops Desk is staffed 24 x 7

        * Telephone at 517-241-8000
        * Email at OperationsLts@michigan.gov
        * LEIN at ELOPS

    3) Through your EM

Use of LEIN notification via PSAP mnemonic

- "PSAP" will send a LEIN message to every PSAP in Michigan and to MSP Ops Center, try to include the following information in your message:
  - Brief description of the current circumstances.
    - Outage/service interruption/service anomalies
  - Identification of back-up PSAP(s) and/or request for back-up PSAP(s) needed.
  - Method to contact PSAP during the outage.
  - Estimated time of duration (if possible).
  - Any other information relevant to the outage that PSAPs and the MSP Ops Desk may need to be aware of. Examples of this may include a request for additional resources, names of departments, or personnel that may need to be contacted on behalf of the PSAP

Communication Provider-Initiated Notice

- A communications provider whose network is affected by an outage should communicate the outage directly to the affected PSAP(s).
- If direct communication is not possible, the provider's information can be disseminated through LEIN via the MSP Ops Desk.
- Information provided should include:
  - The areas affected by the outage.
  - The nature and cause of the outage.
  - Status, including repair progress and expected time of completion.
  - Name and contact information for the person/facility serving as lead on the issue (this is in the event of media inquiries, shift changes, or other contact that may need to be made in regard to the issue).
  - The name and direct contact information for the person with the communications provider who is managing the outage incident.
  - Incident/trouble ticket number, if appropriate.

Restoration

- Restoration notices must be sent to those notified of the outage as soon as possible. These can include:
  - PSAP Management.
  - Back up PSAPs and any mutual aid involved.
  - Public Notification - All systems utilized for initial notification (i.e. EAS, EMnet, Media page, and public notification alert systems such as Nixle and Code Red) as well as any additional media outlets that may have been engaged during the outage.
  - All affected public safety agencies and emergency personnel.
  - MSP Ops Desk (ELOP), if they were notified.
  - A LEIN message to the PSAP mnemonic if an earlier message was sent.

Additional Notifications

- Any updates received should be shared, including “functions restored” message through all original channels when the event is over.
- After normal operations have been restored, the PSAP manager should file a report of the outage as soon as possible with the FCC. This can be done online through the FCC web page at:

  www.fcc.gov/general/public-safety-support-center.
- After normal operations have been restored, the PSAP manager should also file a report of the outage as soon as possible with the State 911 Office. This can be done online through the SNC web page at:

  www.michigan.gov/snc.

TDoS and other interruptions

- A denial of service, although it originally used telephone operations as the hostage by flooding phone lines with auto-dialed calls until ransom was paid, experience is teaching the 911 community that TDoS can take on many forms. Some forms of emergency communication interference events are known and others are yet to be hatched by bad actors.
  - February 2013 – Hackers sent a zombie apocalypse message through the EABS of ten television channels in several different states.
  - October 2016 – A virus was sent through a link on Twitter that infected smart phones. The phone would repeatedly dial 911 unbeknownst to the phone's owner. In areas where there were high numbers of the tweeter's followers, the influx of 911 calls disrupted several PSAPs' operations.
  - April 2017 – While originally believed to be an on-site hack, all 156 of the tornado sirens serving the city of Dallas were activated at the same time (when no weather event was occurring).

TDoS and other interruptions

- What to do?
  - NENA Guidelines (www.NENA.org):
    - Prepare in advance – discuss scenarios, know your system providers' contacts (911 network service, CAD vendor, CPE vendor, radios, etc.).
    - Document the best information you possibly can - times, circumstances, duration, frequency
    - File a complaint with the **Internet Crime Complaint Center** (IC3) - co-sponsored by the Federal Bureau of Investigation (FBI) and the National White Collar Crime Center at **www.ic3.gov.** Include the keywords *TDoS, PSAP,* and *Public Safety* in the description of the incident.
    - File a report with your PSAP's jurisdiction police department.
  - Contact the Michigan Intelligence Operations Center (MIOC) Cyber Security Unit at 877-MI-CYBER (877-642-9237).

TDoS and other interruptions

- What's being done to help?
  - Homeland Security Advanced Research Projects Agency's Cyber Security Division (CSD) is funding two research projects designed to harden defenses against TDoS attacks.
    - Developing a prototype solution for complex TDoS attacks that will use a multi-level filter approach to analyze and assign a threat score to each incoming call in real time. That score will help distinguish legitimate from malicious calls and help mitigate an influx of malicious calls by terminating or redirecting them to a lower priority queue at a partner service to manage the calls.
    - Researching a platform that monitors each incoming call's signaling messages, metadata and voice contents to determine if suspicious. Then prioritize the call according to an analysis of its content and audio to ensure real emergency calls are routed to 911 operators for immediate action. Additionally, the research team has developed a novel approach to check for synthetic voice to identify and address potential TDoS calls generated by phone bots.

Harriet Miller-Brown

State 911 Administrator

517 243 2075

Miller-BrownH@michigan.gov