Protecting Your Center From Ransomware

OVERVIEW

Emergency communications centers (ECC), public safety answering points (PSAP,) and public safety communications centers (PSCC) are often targeted by malicious actors seeking to disrupt 9-1-1 operations and their ability to provide life-saving and critical emergency services to the public. These nefarious actors who launch ransomware attacks prey on a lack of training and cyber awareness, typically spreading through phishing emails or by a victim unknowingly visiting an infected website. These attacks are more than just a nuisance – causing 9-1-1 service degradation or even shutdowns.

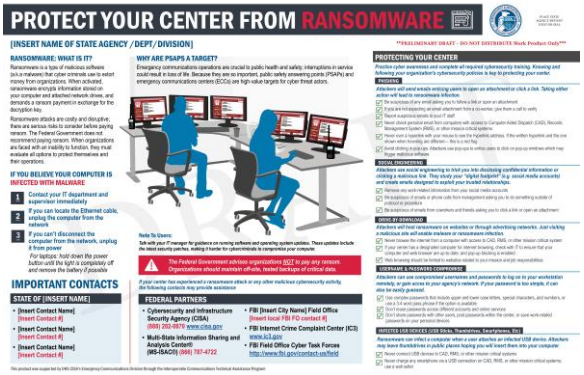
Since ransomware payments do not ensure data will be decrypted or systems or data will no longer be compromised, federal law enforcement do not recommend paying ransom. In addition, the Treasury Department warns these payments run the risk of violating Office of Foreign Assets Control (OFAC) sanctions. Therefore, prevention is key.

PSAP RANSOMWARE POSTER

CISA's Interoperable Communications Technical Assistance Program (ICTAP) designed the CISA PSAP Ransomware Poster to be placed in an ECC, PSAP, PSCC, or 9-1-1 Call or Dispatch Center. It provides information on ways to reduce the risk of ransomware.

The ransomware poster is customizable for ECCs, PSAPs, and PSCCs to fill in agency-specific resources (i.e., the requester's key points of contact), providing stakeholders with a customized product for their agency. It defines ransomware and provides information on:

- Why ECCs, PSAPs, and PSCCs may be targeted
- Specific recommendations on how to protect ECCs, PSAPs, and PSCCs
- Contact information for agency-specific resources and federal partners



CISA PSAP Ransomware Poster

CISA is actively customizing and distributing posters to state and other stakeholder agencies.

To receive an agency specific customized PSAP Ransomware Poster, Statewide Interoperability Coordinators (SWICs), state, local, territory, and tribal points of contact can contact their CISA Emergency Communications Coordinator or email ecd@cisa.dhs.gov. Requests should include the following:

a) Name of State Agency/Dept/Division (Top left side of poster)
b) High Resolution PNG or JPEG file (Top right corner of poster)
c) Important State Office Contacts (Bottom left corner of poster; up to three contacts)
d) FBI Field Office Contact information (Bottom center under Federal Partners)
e) Point of Contact for the Request (Who can be contacted if additional information is required?)

SWICs, state, local, territory, and tribal points of contact may request up to 10 printed 20"x 30" copies of the poster and an electronic file will be provided for printing additional copies. For more information on CISA's ICTAP services, visit cisa.gov/safecom/ictapscip-resources or other 911 resources, visit cisa.gov/safecom/next-generation-911.

For more information and resources on the ransomware, visit cisa.gov/ransomware.