ALABAMA 911 BOARD

April 26, 2022
Talk About It Tuesday!

Introduction & Contact Information

Leah Missildine
Executive Director for the Alabama 9-1-1 Board
Email: leah@al911board.com

Dana Nation
Program Coordinator for the Alabama 9-1-1 Board
Email: dana@al911board.com

Michelle Peel
Program Coordinator for the Alabama 9-1-1 Board
Email: michelle@al911board.com

Jamie Ginn
President, OTMCyber
Email: jginn@otmcyber.com
Tel: 253-514-5695

Agenda
April 26, 2022

- CISA's Cybersecurity Resources
- Upcoming Training Opportunities

Who is CISA?

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CISA Plays Two Key Roles

We Are the Operational Lead for Federal Cybersecurity, or the Federal "dot gov"

CISA acts as the quarterback for the federal cybersecurity team, protecting and defending the home front—our federal civilian government networks—in close partnership with the Office of Management and Budget, which is responsible federal cyber security overall. CISA also coordinates the execution of our national cyber defense, leading asset response for significant cyber incidents and ensures that timely and actionable information is shared across federal and non-federal and private sector partners.

We Are the National Coordinator for Critical Infrastructure Security and Resilience

We look at the entire threat picture and work with partners across government and industry to defend against today's threats while securing the nation's critical infrastructure against threats that are just over the horizon.

https://www.cisa.gov/about-cisa

Who is SAFECOM?

SAFECOM was formed in 2001 after the terrorist attacks of September 11, 2001 as part of the Presidential E-Government Initiative to improve public safety interoperability, allowing emergency responders to communicate effectively before, during, and after emergencies and disasters. SAFECOM's mission is to improve designated emergency response providers' inter-jurisdictional and inter-disciplinary emergency communications interoperability through collaboration with emergency responders across federal, state, local, tribal, and territorial governments, and international borders.

Public safety and emergency communications is an ever-changing field in which practitioners must stand ready to face new challenges. SAFECOM endeavors to assist the public safety community in navigating changes to the emergency communications ecosystem.

https://www.cisa.gov/safecom/about-safecom

Why 9-1-1 centers?

NG911 systems enhance the capabilities of today's 911 networks, allowing more types of communication and establishing a level of resiliency not previously possible. NG911 allows 911 centers to accept and process a range of information from responders and the public, including text, images, video, and voice calls.

What does this have to do with cybersecurity? The legacy 9-1-1 system had relatively few means of entry for attacks. All this technology of NG911 allows for new avenues of attack. These risks present a new level of exposure that PSAP administrators must understand and actively manage.

9-1-1 centers become targets because they are critical to public safety. A 9-1-1 center cannot afford to be down. Hackers know this and attempt to exploit it. Redundancy as well as other procedures to protect against a cyber attack are crucial.

What does this mean for you?

No matter what your position in a PSAP or Emergency Communications District, you need to educate yourself on the vulnerabilities of the equipment you use everyday. If you are a supervisor, manager, or director, you need to educate yourself on the vulnerabilities of the equipment your reports use as well. All of you need to work together to develop a culture of security and a cybersecurity plan that focuses on prevention and ensures the IT infrastructure is protected. Regular training and review of plan is needed also. CISA's resources are a great start.

CISA's Resources

There are many ways to protect your 9-1-1 center. The first step is educating yourself and your staff. Work with your IT department to establish or update procedures and mandate regarding a variety of cyber threat.

CISA has a variety of resources. The first covers Cyber Risks to NG911.

https://www.cisa.gov/sites/default/files/publications/NG911%20Cybersecurity%20Primer.pdf

Another resource covers Denial of Service Attacks.

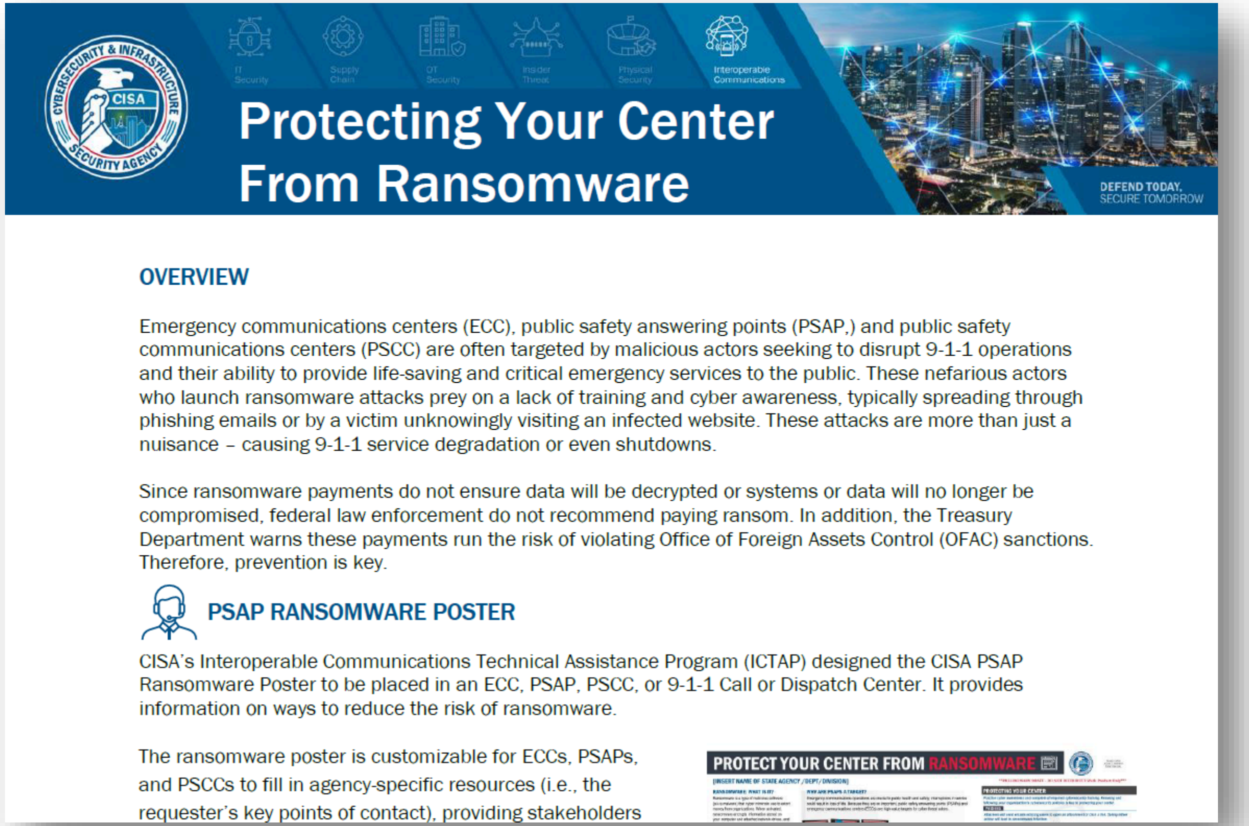
https://www.cisa.gov/sites/default/files/publications/Cyber%20Risks%20to%20911%20TDoS_6.4.2020%20-%20%28508c%29_1.pdf

They have an extensive site dedicated to ransomware.

https://www.cisa.gov/stopransomware

CISA Ransomware Poster

Protect Your Center from Ransomware Poster


CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
CISA
IT Security
Supply Chain
OT Security
Insider Threat
Physical Security
Interoperable Communications
DEFEND TODAY. SECURE TOMORROW

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.

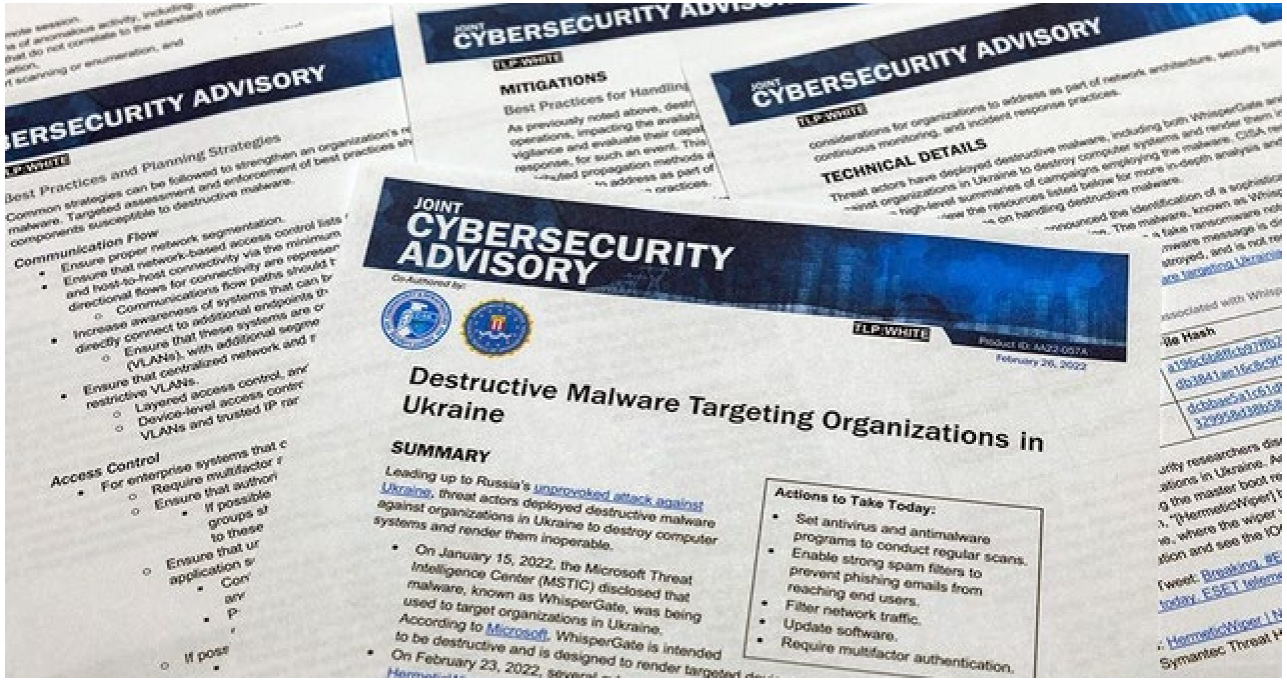
The ransomware poster is customizable for ECCs, PSAPs, and PSCCs to fill in agency-specific resources (i.e., the requester's key points of contact), providing stakeholders

Case Studies Available

- Malware Attacks: Lessons Learned from an ECC highlights the experience of a local ECC with a malware attack, which impacted their computer-aided dispatch (CAD) system, and lessons learned from this event.
- Telephony Denial of Service (TDoS) Attacks: Lessons Learned from a PSAP showcases a local PSAP's experience with a multi-year TDoS attack and the actions they took to protect their center.
- Cyber Incident Response to PSAPs: A State's Perspective provides insight to state-level responses to a cyber incident at a PSAP and shares their lessons learned from these responses.

How can we prepare for a Russian cyberattack?

https://thehill.com/opinion/cybersecurity/3460074-a-russian-cyberattack-is-coming-both-lawmakers-and-citizens-must-prepare/



JOINT CYBERSECURITY ADVISORY

Co-Authored by:

TLP:WHITE

Product ID: AA22-057A

February 26, 2022

Destructive Malware Targeting Organizations in Ukraine

SUMMARY

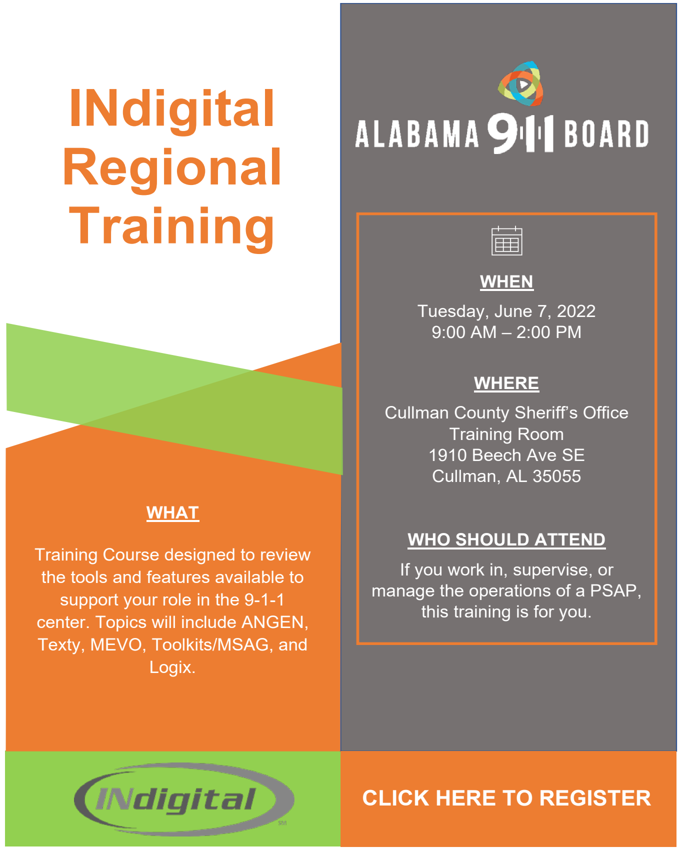
Leading up to Russia's unprovoked attack against Ukraine, threat actors deployed destructive malware against organizations in Ukraine to destroy computer systems and render them inoperable.

- On January 15, 2022, the Microsoft Threat Intelligence Center (MSTIC) disclosed that malware, known as WhisperGate, was being used to target organizations in Ukraine. According to Microsoft, WhisperGate is intended to be destructive and is designed to render targeted dev
- On February 23, 2022, several

Actions to Take Today:

- Set antivirus and antimalware programs to conduct regular scans.
- Enable strong spam filters to prevent phishing emails from reaching end users.
- Filter network traffic.
- Update software.
- Require multifactor authentication.

Upcoming Training



INdigital Regional Training

ALABAMA 911 BOARD

WHEN

Tuesday, June 7, 2022
9:00 AM – 2:00 PM

WHERE

Cullman County Sheriff's Office
Training Room
1910 Beech Ave SE
Cullman, AL 35055

WHO SHOULD ATTEND

If you work in, supervise, or manage the operations of a PSAP, this training is for you.

WHAT

Training Course designed to review the tools and features available to support your role in the 9-1-1 center. Topics will include ANGEN, Texty, MEVO, Toolkits/MSAG, and Logix.

INdigital

CLICK HERE TO REGISTER

- June 7, 2022 – Cullman County Sheriff's Office
- June 8, 2022 – Tuscaloosa County 9-1-1
- August 16, 2022 – Alexander City
- August 17, 2022 – Pike County Lake
- September 13, 2022 – Mobile County Communications District
- September 29, 2022 – Homewood Police Department

'22 ALABAMA 911 BOARD USER CONFERENCE

Questions

Leah Missildine
Executive Director for the Alabama 9-1-1 Board
Email: leah@al911board.com

Adam Brown
Deputy Director for the Alabama 9-1-1 Board
Email: adam@al911board.com

Dana Nation
Program Coordinator for the Alabama 9-1-1 Board
Email: dana@al911board.com

Michelle Peel
Program Coordinator for the Alabama 9-1-1 Board
Email: michelle@al911board.com

Jamie Ginn
President, OTMCyber
Email: jginn@otmcyber.com
Tel: 253-514-5695

Phone: 334.440.7911