PSAP CYBERSECURITY AWARENESS WEBINAR

Registering Your Attendance

- Please send an email to the following people to confirm your attendance:

darinanderson@nd.gov

awhite@lafayettegroup.com (if you want the handouts after the sesion)

Program Sections

I. Program Intro & Overview

II. Why PSAPs are a Target

III. Types of Threat Attacks

IV. Specialized Attack Situations – Examples & Protection

Program Sections *(continued)*

VI. Cyber Hygiene & Overall Best Practices

VII. Responding To & Reporting Cyberattacks

VIII. Okay, Where Do I Start?

IX. Closing Comments

Webinar “Ground Rules”

- Copies of slides and a handout with supplemental resources will be provided
- Ask questions by “raising hand” or putting them in the chat section
- What we mean by PSAPs (includes ECCs)
- Any slide with a green background is a Best Practice recommendation

SECTION I – PROGRAM INTRO & OVERVIEW

Recent Attack Examples

- **December 2021:** Multiple PSAPs across the nation were unable to process payroll after their cloud-hosted timekeeping solution was hit by ransomware
- **September 2021:** Large Texas Metropolitan area center hit with TDoS attack against 9-1-1. Over 1,800 calls.
- **Summer 2021:** Hospital phone system hacked in the Southeast. Hundreds of 9-1-1 calls launched against local PSAP
- **January 2021:** Multiple PSAPS were compromised by a vulnerable e-mail server with access to both the Internet and the ESINet

How PSAP Technology Has Changed

Dispatch/PSAP technology used to be simple telephones and radios that presented almost no cybersecurity risk

Today's technology is almost completely computerized and interconnected, creating significant cybersecurity risk

What Is Their Motive?

- **Disruption –** Cyberattacks may shut down public access to 9-1-1, leading to public confusion and disrupting the dispatch of First Responders
- **Ransom –** As the networks, data and services are vital to public safety, PSAPs are more likely to pay a Bitcoin ransom in order to restore service
- **Lack of Defenses –** PSAPs, municipalities, may not have a strong cyber defense system – especially when compared to other targets
- **Collateral Damage –** Victim of Lateral Attack

The Potential Cyberattack Impact

- TDoS May Prevent the Public From Reaching 9-1-1 or the 10 Digit Admin Line
- CAD or Records Systems encrypted- no access
- Delay in Dispatching First Responders
- Destroying evidence, such as body camera footage
- Financial loss

Why This Webinar Was Developed

- Attacks are on the rise and can have a devastating effect on the primary mission of the PSAP
- Webinar serves as awareness education and is part of a larger education/protection program
- Provides threat preparedness and response suggestions

SECTION II – WHY PSAPS ARE VULNERABLE TO ATTACKS

PSAP Cybersecurity

Defending:

- 9-1-1 Call Handling
- CAD
- Radio
- Records
- Critical Systems

Risk Level Increases With NG9-1-1

- NG911 is different from traditional systems:
  - Requires standardized identity management and credentialing across systems
  - Introduces new attack vectors
  - Possible to launch multiple distributed attacks with greater automation from a broader geography against more targets

Why Is The Public Sector A Target?

- **Willingness To Pay The Ransom –**
  - PSAPs are critical to the effective delivery of life-saving public safety services
  - Desire to avoid negatively publicity and loss of public confidence
  - Agencies are frequently tasked with providing services to citizens with limited access to technical and cybersecurity resources

What Is “Cyber Reflection” a.k.a Hacktivism?

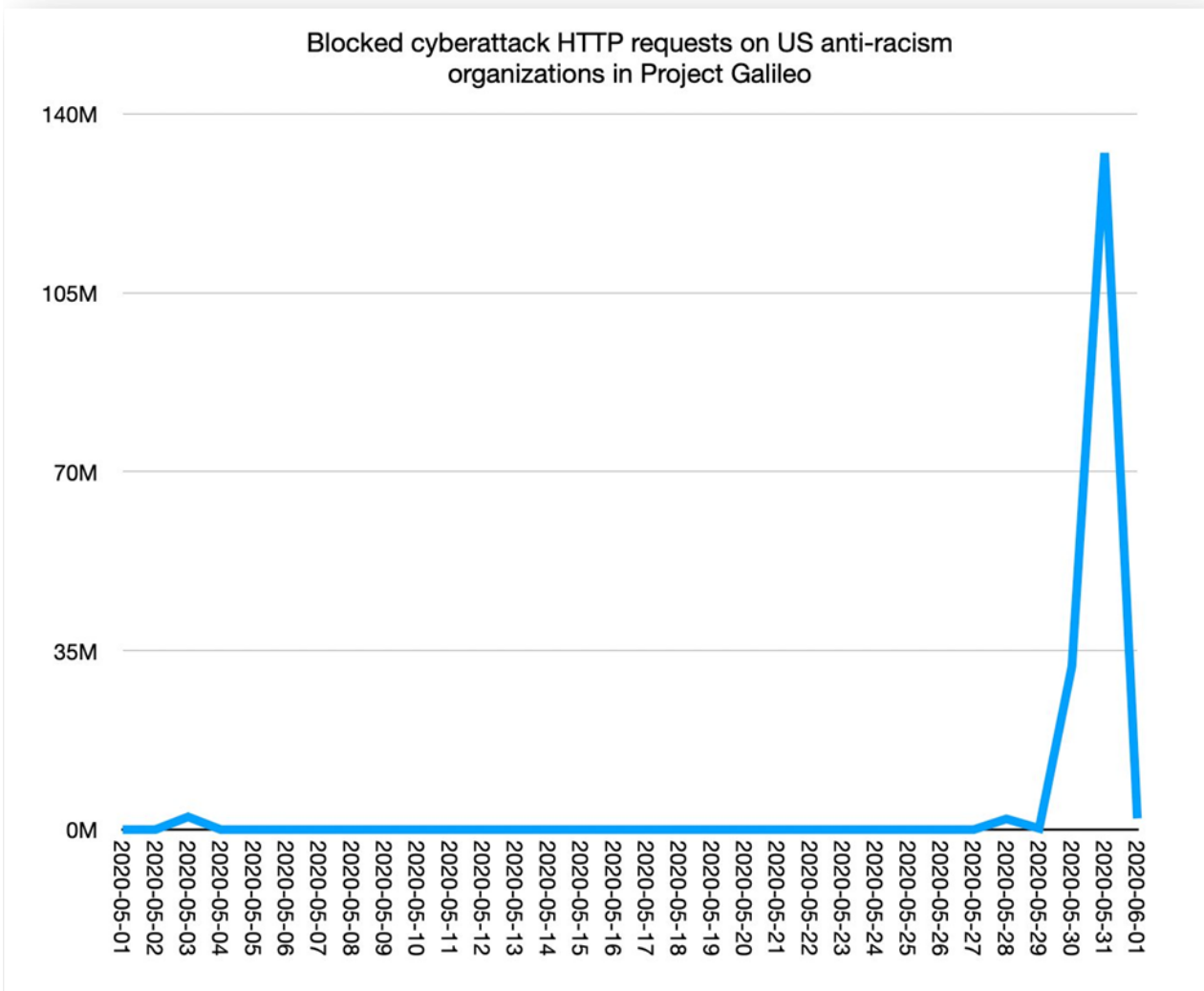
- For every geopolitical protest you see happening in-person, there’s a reflection associated with that demonstration happening in cyberspace
- Just as people protest in-person, many times they also protest in cyberspace

Cyberattacks During Civil Unrest – Why?

- **Disruption –** Cyberattacks may shut down public access to 9-1-1, leading to public confusion and disrupting dispatch
- **Disinformation –** Spreading false or misleading information about the events or situation
- **Loss of Confidence –** If citizens are unable to connect with law enforcement/PSAP, they will lose confidence and may take matters into their own hands

Cyberattacks During Civil Unrest – How?

- Almost exclusively, these have been TDoS/DDoS Attacks



Cyberattacks During Civil Unrest – Examples

- Minneapolis was the target of a cyberattack while protests fueled by the police killing of George Floyd were also underway
- Ferguson (MO) Police Department website and email after Michael Brown shooting
- Baltimore city website and other government systems after Freddy Brown shooting
- Anonymous Returns In The Wake Of Civil Unrest In The US

Defending Against Attacks During Civil Unrest

Over the rest of this presentation, we will discuss:

- Why PSAPs should enroll in a DoS protection service capable of detecting abnormal traffic flows and redirects them away from your network
- Why antivirus software is important to keep systems secure
- Example security practices that help minimize the risk of outside access to your information
- Creating a plan to ensure successful and efficient communication, mitigation, and recovery should an attack occur

SECTION III – TYPES OF ATTACK THREATS

Types of PSAP Cyberattacks

1. **Direct TDoS Attack Against 9-1-1 and Admin Phone Lines**
2. **Phishing – Over 90% of successful attacks**
3. **Indirect Attack – Lateral, Ransomware, etc.**
4. **Remote Access to Systems**

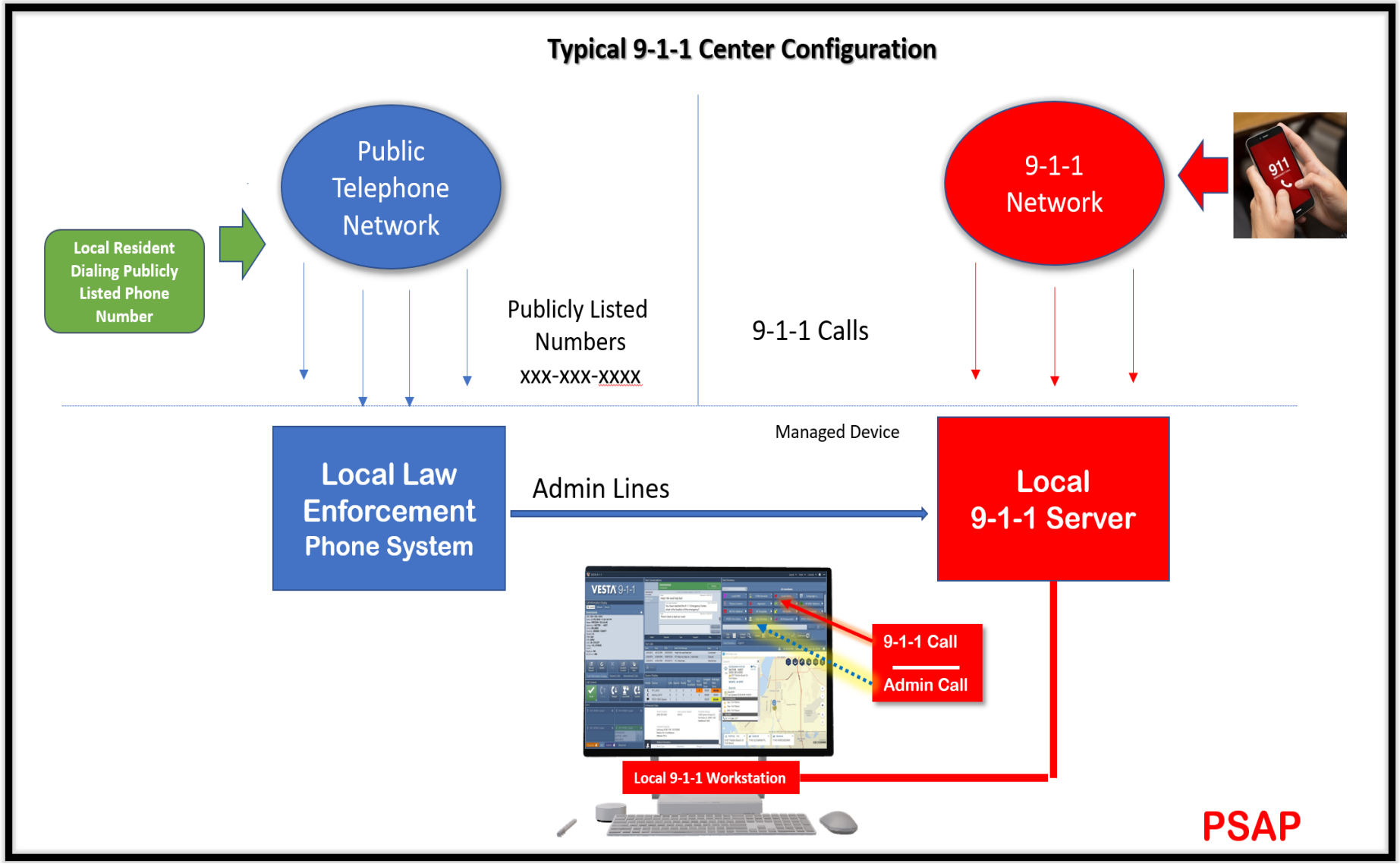
Attacks Against PSAPs and Admin Phone Lines

- *Telephony Denial of Service (TDoS)*

Denial Of Service Attacks (DoS)

- An attempt to exhaust resources available to a network or server and interrupt access to genuine users (such as 9-1-1)
- One of the oldest forms of cyberattacks
- TDoS is the voice communications version of DDoS

Typical 9-1-1 Center



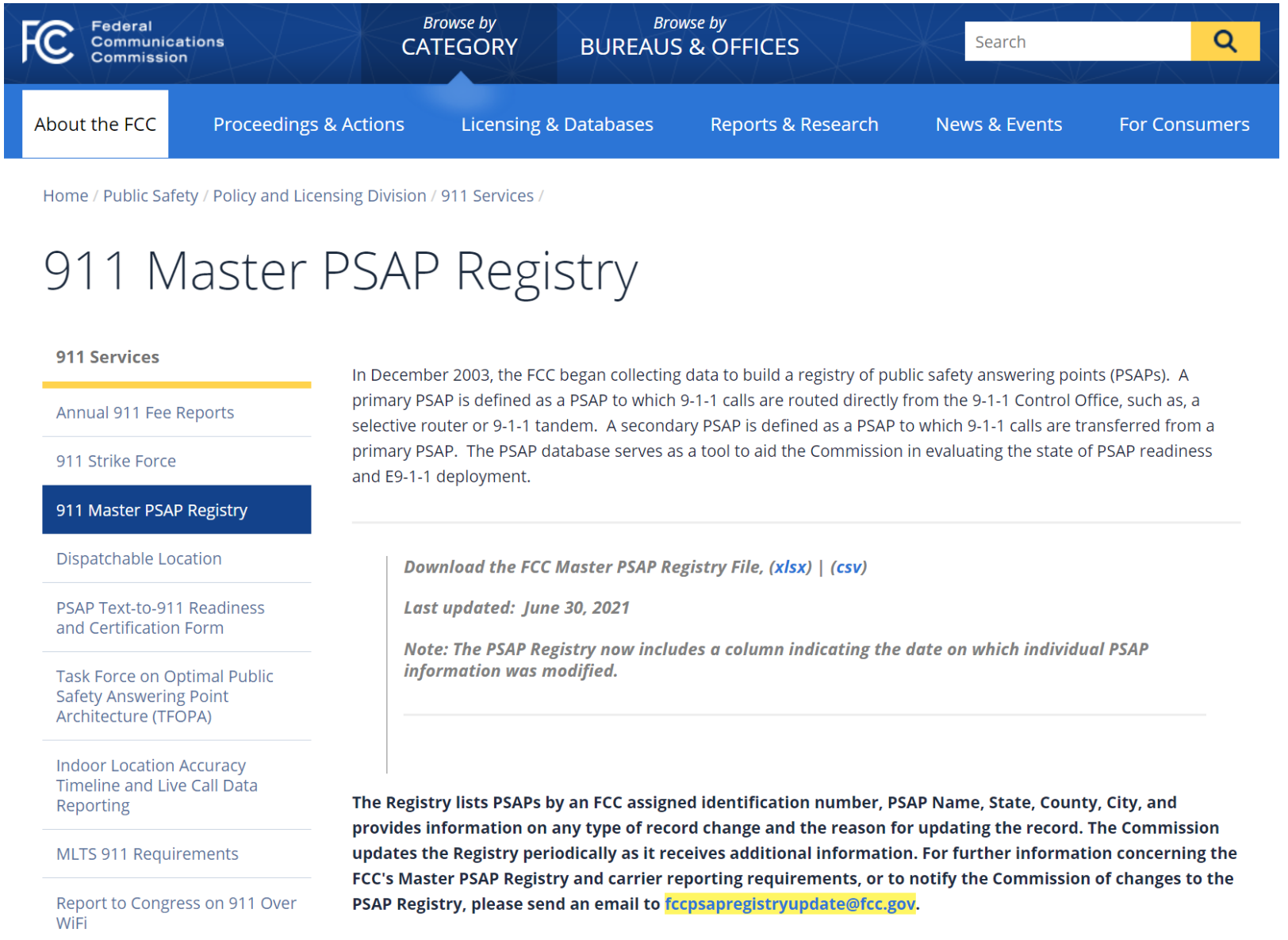
Example – TDoS Attacks in Florida

- Actors are located in the Gaza Strip
- Attacked PSAPs in numerous states in 2019
- Attacks resumed in July 2020
- Thousands of Calls- attack can last hours or days

Attack Methods:

- Dialing- Hang Up on PSAP Answer
- Conference PSAPs Together
- Verbal Threats to Call Takers

PSAP Locations Are Available Online



Federal Communications Commission

Browse by CATEGORY | Browse by BUREAUS & OFFICES | Search

About the FCC | Proceedings & Actions | Licensing & Databases | Reports & Research | News & Events | For Consumers

Home / Public Safety / Policy and Licensing Division / 911 Services /

911 Master PSAP Registry

911 Services

- Annual 911 Fee Reports
- 911 Strike Force
- 911 Master PSAP Registry
- Dispatchable Location
- PSAP Text-to-911 Readiness and Certification Form
- Task Force on Optimal Public Safety Answering Point Architecture (TFOPA)
- Indoor Location Accuracy Timeline and Live Call Data Reporting
- MLTS 911 Requirements
- Report to Congress on 911 Over WiFi

In December 2003, the FCC began collecting data to build a registry of public safety answering points (PSAPs). A primary PSAP is defined as a PSAP to which 9-1-1 calls are routed directly from the 9-1-1 Control Office, such as, a selective router or 9-1-1 tandem. A secondary PSAP is defined as a PSAP to which 9-1-1 calls are transferred from a primary PSAP. The PSAP database serves as a tool to aid the Commission in evaluating the state of PSAP readiness and E9-1-1 deployment.

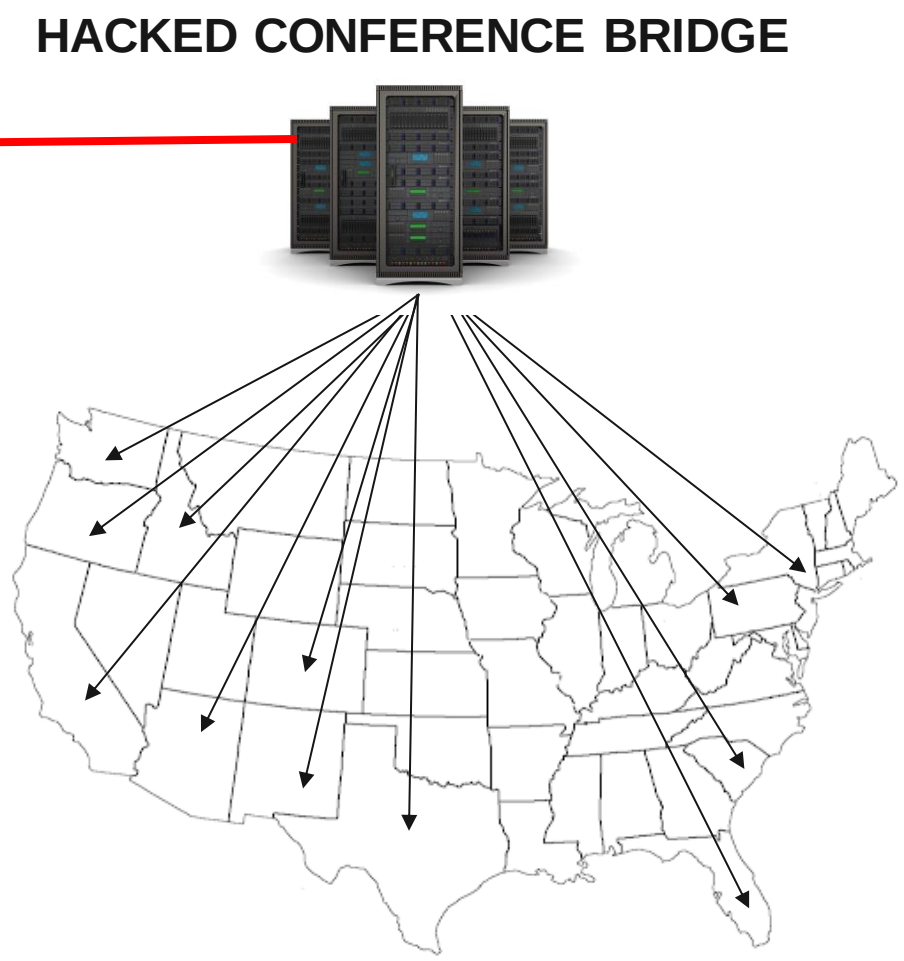
Download the FCC Master PSAP Registry File, (xlsx) | (csv)

Last updated: June 30, 2021

Note: The PSAP Registry now includes a column indicating the date on which individual PSAP information was modified.

The Registry lists PSAPs by an FCC assigned identification number, PSAP Name, State, County, City, and provides information on any type of record change and the reason for updating the record. The Commission updates the Registry periodically as it receives additional information. For further information concerning the FCC's Master PSAP Registry and carrier reporting requirements, or to notify the Commission of changes to the PSAP Registry, please send an email to fccpsapregistryupdate@fcc.gov.

Telephony Denial of Service (TDoS)- Admin Lines

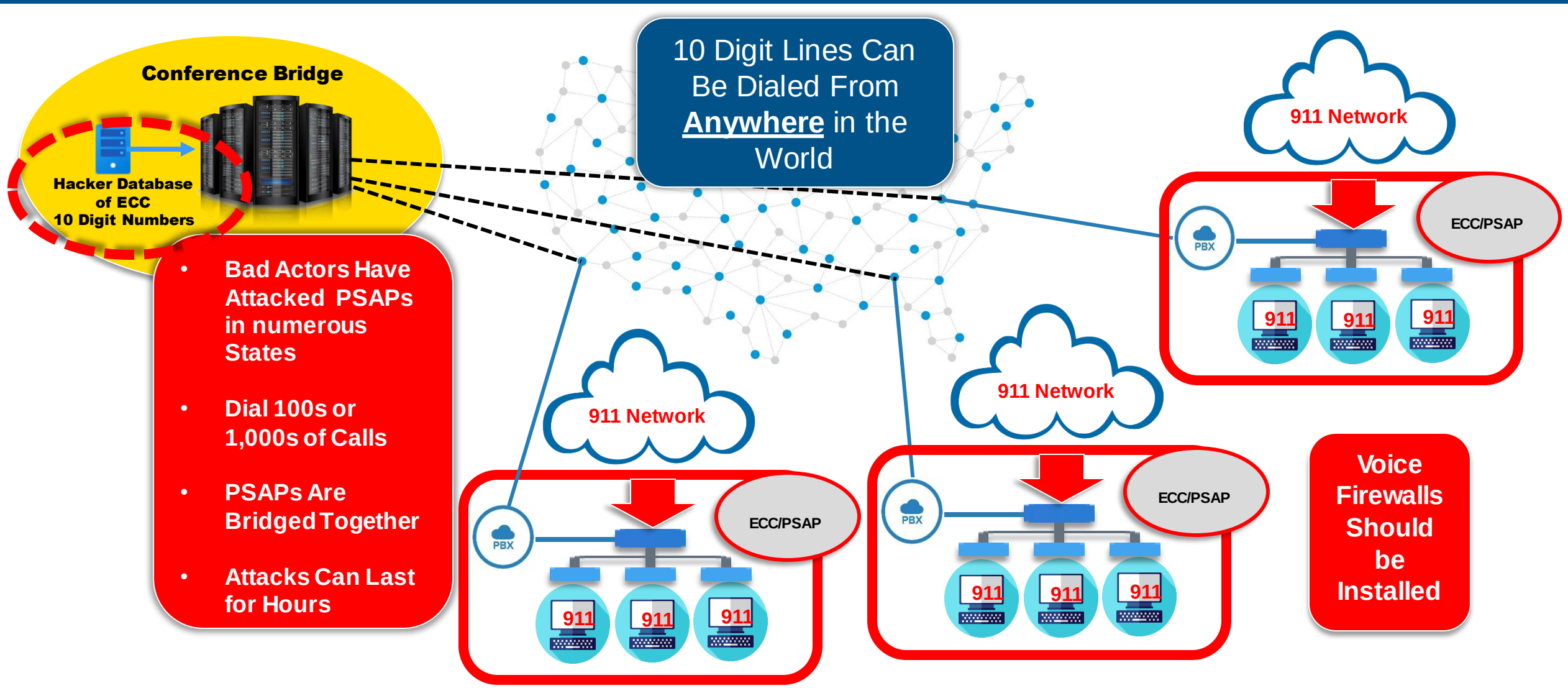


1. Browse the web for sheriff/police department phone numbers

2. Load these numbers into ‘hacked’ conference bridge

3. Direct the conference bridge to dials targets continuously, connecting call takers via the bridge

TDoS Attack – Admin Lines – Multiple PSAPs



Industry Best Practice-TDoS Appliance

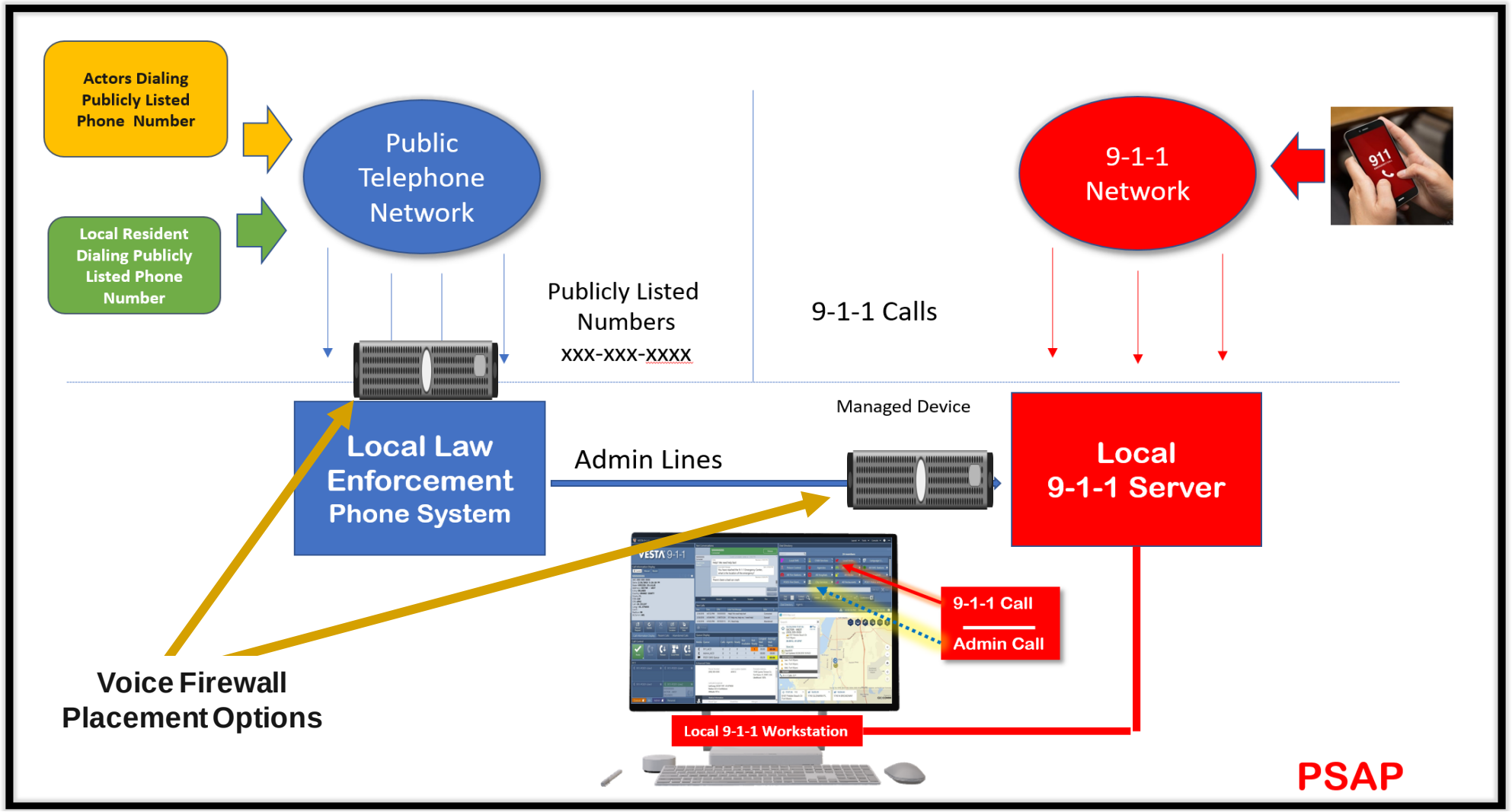
Industry Examples

- Military Bases
- Healthcare: Hospitals
- Financial: Banking
- Call Centers

Recommendations

- TDoS Appliance Should be Installed on Admin Lines at PSAPs
- Provides Call Authentication-Stir/Shaken
- Protection against Robo Calls

Protecting Admin Lines



Attacks Against PSAPs on 9-1-1 Lines

- *Telephony Denial of Service (TDoS)*

Protections Against Erroneous Blocking

FEDERAL REGISTER
The Daily Journal of the United States Government

September 2020
AGENCY: FCC

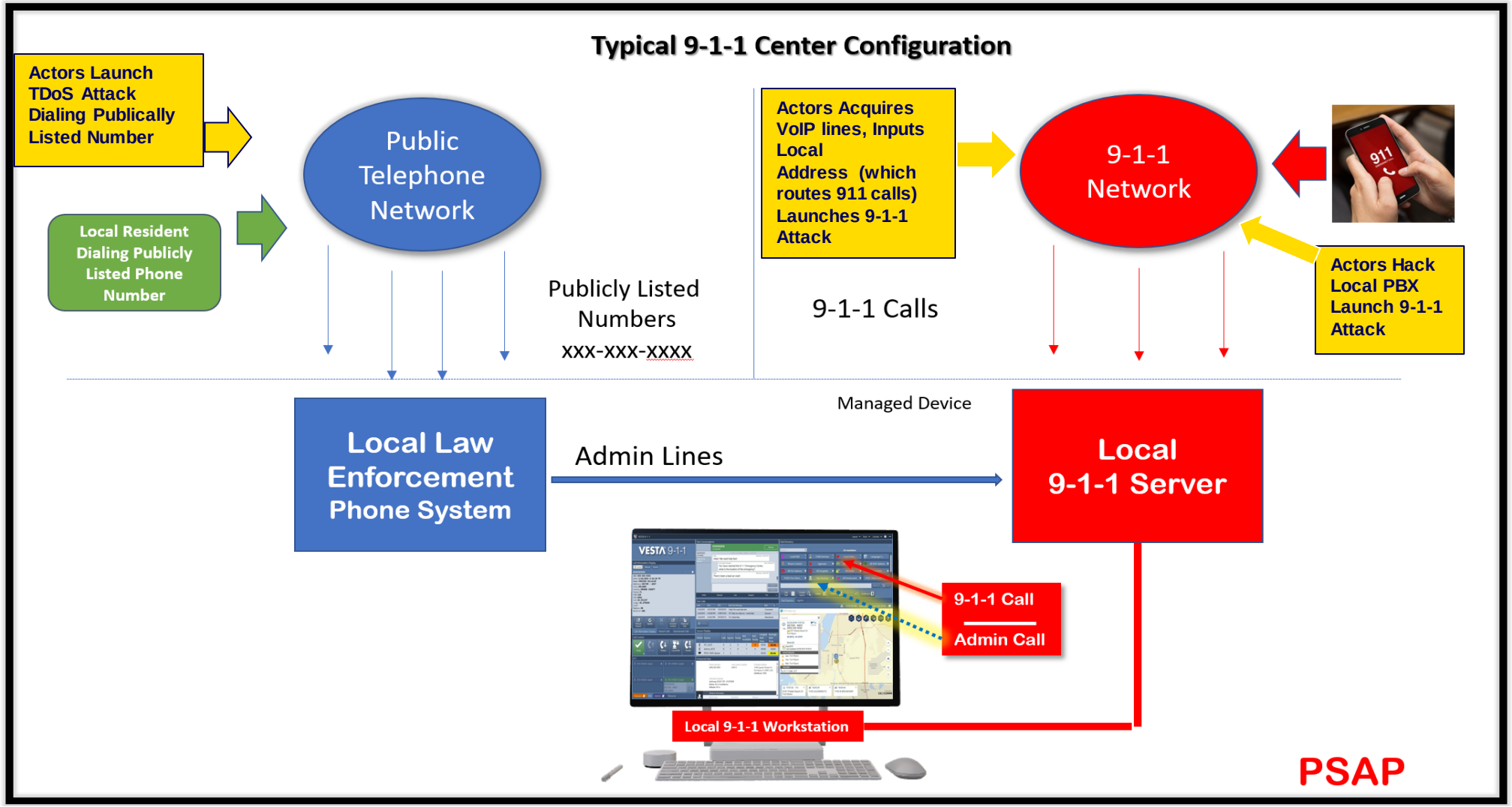
ACTION: Final rule

Calls to PSAPs via **911** are also extremely important and the **FCC makes clear that 9-1-1 calls should never be blocked unless the voice service provider knows without a doubt that the calls are unlawful.**

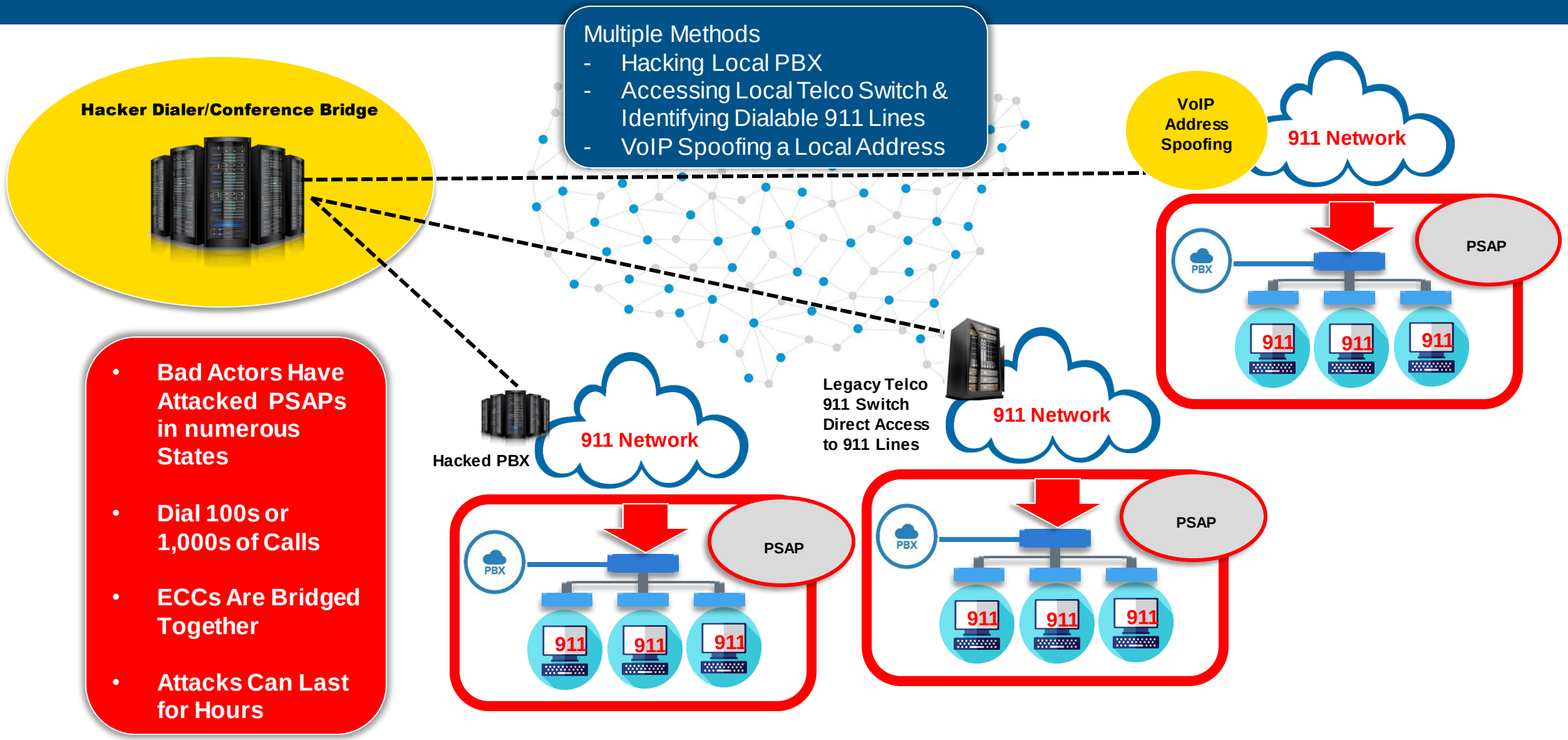
Though some unwanted and illegal calls may reach 911 call centers…

"The FCC believes that 911 call centers themselves are best equipped to determine how to handle the calls they receive."

TDoS- Joint Attack on Admin and 9-1-1



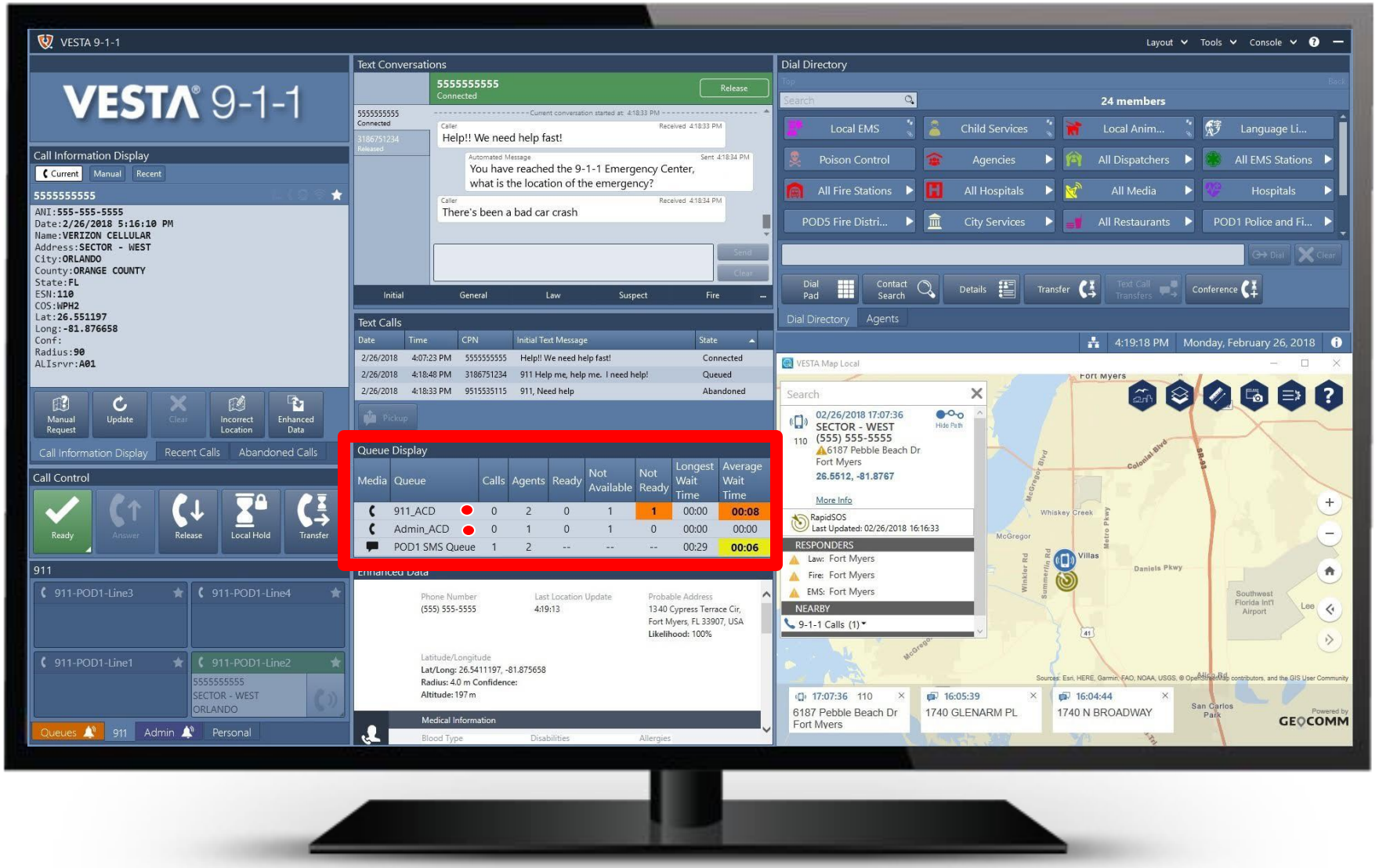
TDoS Attack- 911 Lines- Multiple PSAPs



9-1-1 During a TDoS Attack

- Routing to specific workstations
  - Based on information in call details
  - Establish separate group of workstations
  - If you have a relationship with the carrier they may be able to help with routing changes at their level

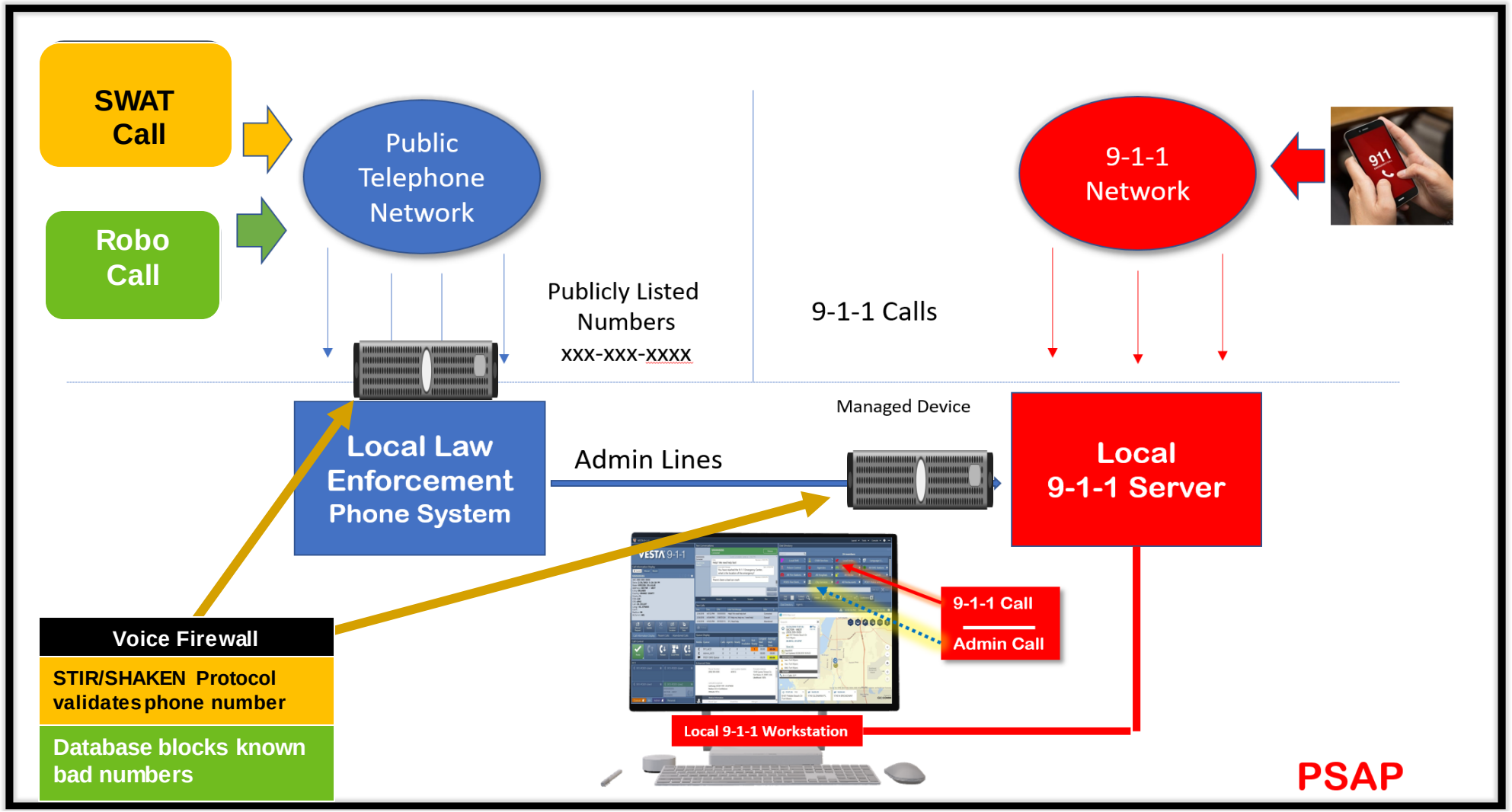
Recognizing TDoS From the CAD Interface



SWATTING

- Follows a common pattern
- Reported incidents prompt a significant law enforcement response
- Presents significant risk to person "SWATTED" as well as the responders
- May be used to distract police while another crime is being perpetrated

Protecting Admin Lines



Phishing

- *Email*
- *Social Media*

Remote Workers Ignore Security Risks

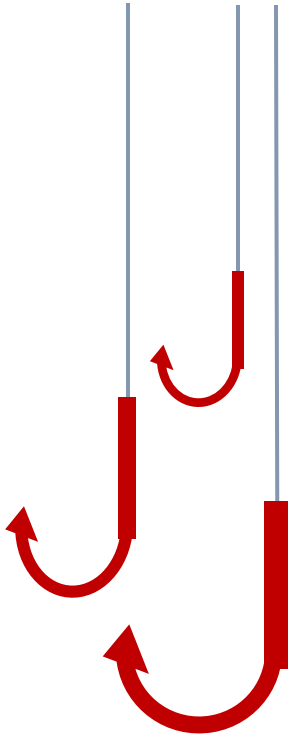
- Poll of over 1,000 remote workers
- Although 96% said they were aware of the risks of clicking through on malicious phishing links, nearly half (45%) open emails they consider to be suspicious
- Nearly half (45%) also admitted to not reporting such emails to their IT security teams

What Is Social Engineering?

- The term used for a broad range of malicious activities accomplished through human interactions
- It uses psychological manipulation to trick users into making security mistakes that they would not normally do or giving away sensitive information
- **How do they get people to "bite"?**
  - Urgency/Time Sensitive – Urgent requirement
  - Scarcity – You'll lose out on something if you don't act quickly
  - Personal Health or Importance – Update on virus in your agency or community

What is Phishing?

"Phishing is the attempt to obtain sensitive information such as usernames, passwords, and credit card details, often for malicious reasons, by disguising as a trustworthy entity in an electronic communication[1]"



Accounts for ~90% of successful cyberattacks

Phishing

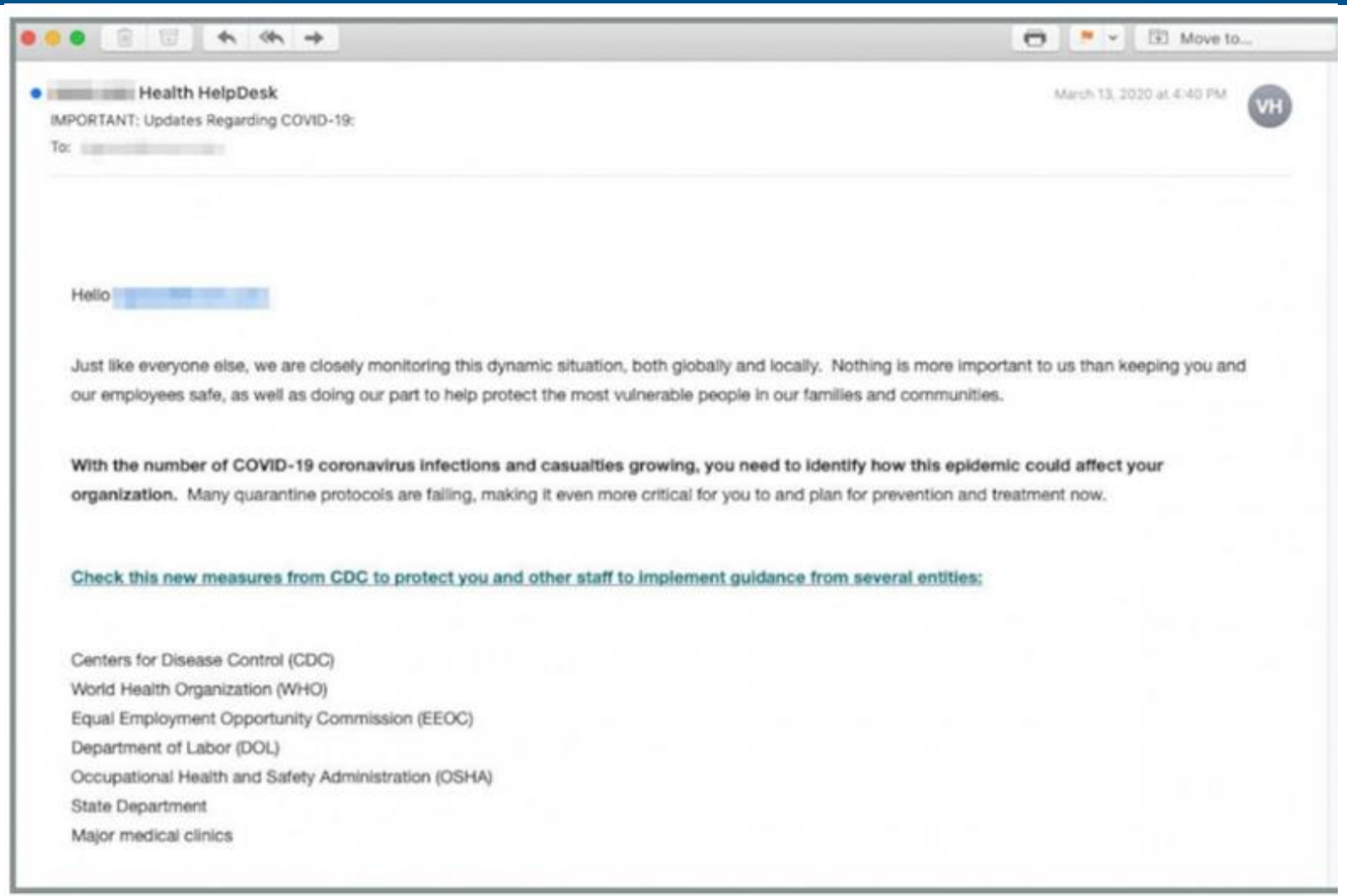
- **Spear Phishing** – Phishing messages crafted specifically for an individual target or group
- **Whaling** – Spear-phishing targeted at high-level, high-value employees
- **Clone Phishing** – Previous legitimate previously delivered online correspondence used to create a clone email

COVID-19 – Cybersecurity/Phishing

- Criminals are using the pandemic to launch cyberattacks by spoofing organizations that are providing COVID-19 updates to the public
- Not a significant increase in the total volume of phishing attempts, just that the focus has shifted to Coronavirus
- People are very nervous about the virus, are multi-tasking and may have a lot of distractions at home – increases vulnerability
- Employees working from home don't have the same protections they had while working in their office
- According to Proofpoint, more than 30% of compromised emails are delivered on Monday as hackers try to capitalize on weekend backlogs

CDC Spoofed Email

Could include that the coronavirus has “officially become airborne” and there “have been confirmed cases of the disease in your location.”



Cybersecurity experts have identified a significant uptick in coronavirus-related phishing scams.
Courtesy of INKY

How Spear Phishing Typically Works

Spear phishing messages appear to be sent from an identity - an individual or a brand - that is known and trusted by the recipient.

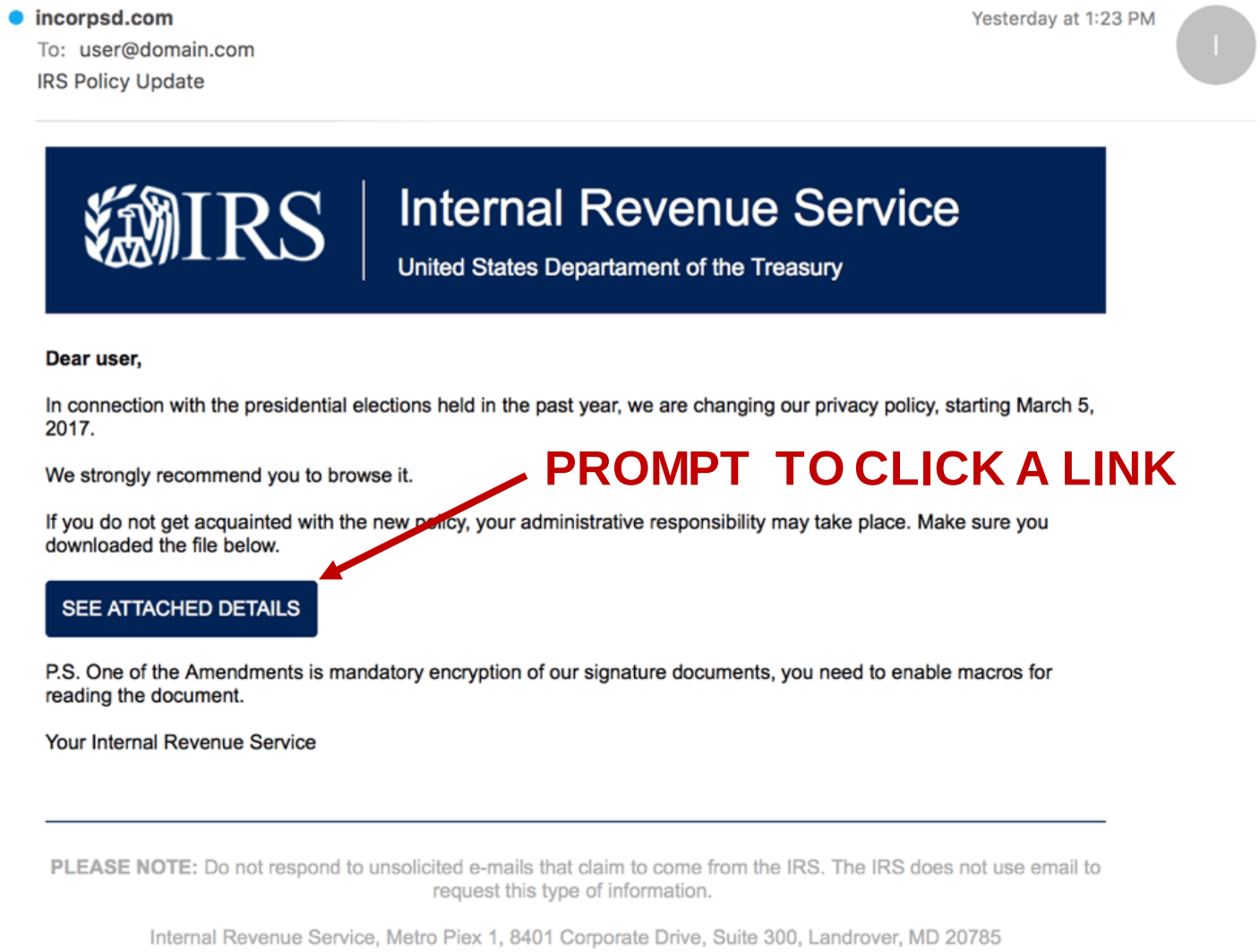
Hacker Identifies a Target & Researches the Victim

Hacker Sends a Targeted, Legitimate Looking Email

Victim Opens an Email Containing Malware

Hacker Uses Access To Steal Data From Victims Computer or Network

Phishing Sample E-mail



incorpsd.com
To: user@domain.com
IRS Policy Update

Yesterday at 1:23 PM

IRS | Internal Revenue Service
United States Departament of the Treasury

Dear user,

In connection with the presidential elections held in the past year, we are changing our privacy policy, starting March 5, 2017.

We strongly recommend you to browse it.

If you do not get acquainted with the new policy, your administrative responsibility may take place. Make sure you downloaded the file below.

SEE ATTACHED DETAILS

P.S. One of the Amendments is mandatory encryption of our signature documents, you need to enable macros for reading the document.

Your Internal Revenue Service

PROMPT TO CLICK A LINK

PLEASE NOTE: Do not respond to unsolicited e-mails that claim to come from the IRS. The IRS does not use email to request this type of information.

Internal Revenue Service, Metro Piex 1, 8401 Corporate Drive, Suite 300, Landrover, MD 20785

Phishing Examples

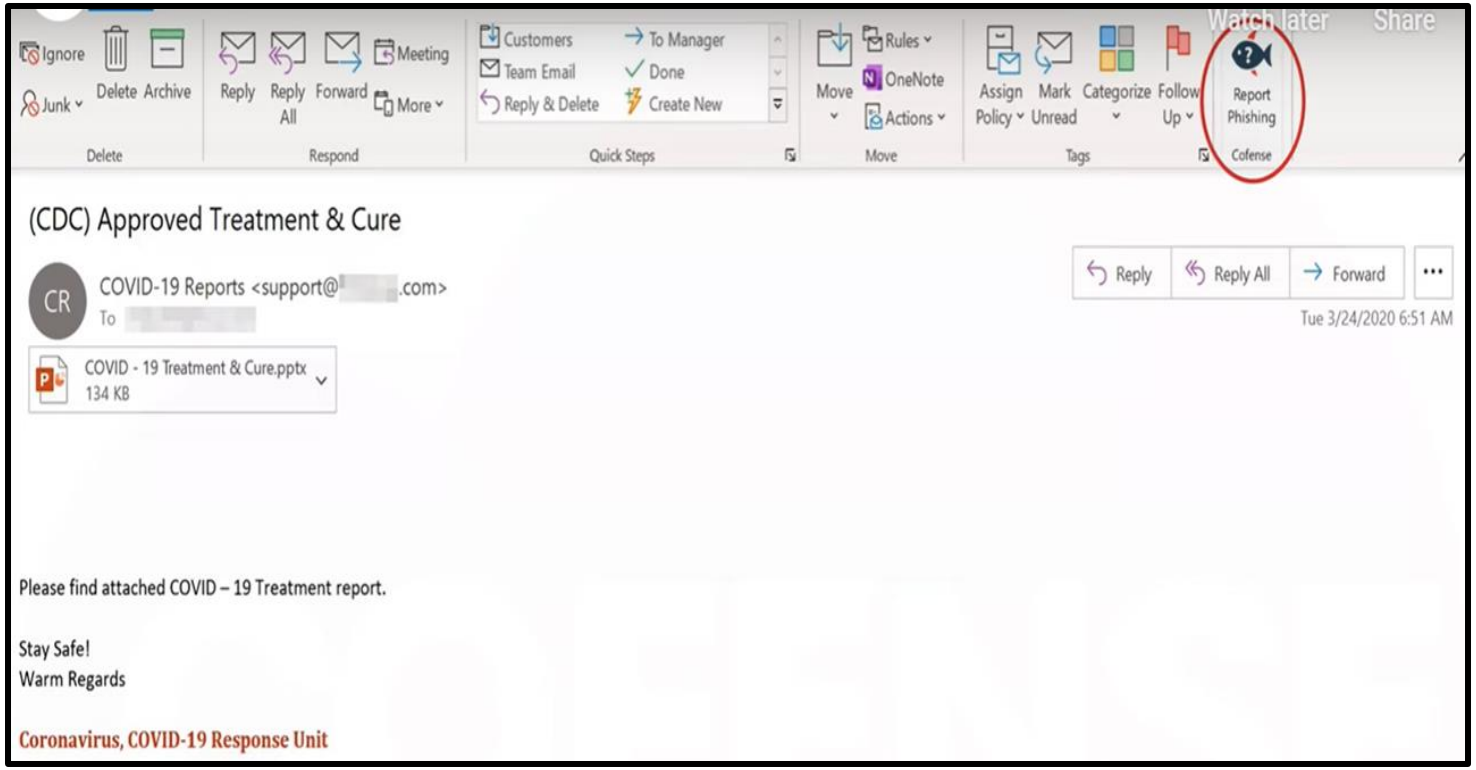
- **False e-mail addresses** — *john.smith@fairfax-va.com*
  ITmanager@cityofbaltimore.com
- **Fake URLs & hyperlinks** — *http://cityofbaltimore911.com/login/unlock.html*
  Click Here
- **"Urgent problem" messages** — *Your password has expired and must be reset immediately. Click Here to reset your login*
- **Illegal activity scares** — *Warning: your account has been suspended for policy violation—xxxadult sites. Contact your IT manager for more information*
- **Unclaimed Prizes** — *Congratulations! You have been selected to receive a $50 amazon gift card. Click Here to claim your valued customer reward*

Credential Theft

- 75% of phishing attacks are aimed at obtaining the user's credentials
- Link directs user to what appears to be a legitimate MS Outlook sign-on screen, so user enters credentials
- Credentials are harvested and then user is routed to the correct site

Fake/Infected Attachments

Instead of a link, they use a document attachment that might be a PDF, Microsoft Word, or other common type of file



Best Practices – Phishing

- Implement a cybersecurity user awareness and training program
- Include guidance on how to identify and report suspicious activity (e.g., phishing) or incidents
- Conduct organization-wide phishing tests to gauge user awareness
- Reinforce the importance of identifying and reporting on potentially malicious emails
- Reminders to Staff that Clicking on *Links* May Be Dangerous

SOCIAL MEDIA AND PERSONAL EMAIL IN YOUR PSAP

Personal Email Use – Same Concerns

Phishing is the major concern

Social Media & Personal Email Access

Do Not Allow:

- Social Media
- Personal Web-Based email

on the PSAP Network

Indirect or Outside Attack Not on the 9-1-1 System

- *Ransomware*
- *Lateral Attacks*
- *Cryptojacking*
- *USB drives*

Ransomware

- **Ransom: Money demanded for releasing captive + Ware: reference to software/files**

- A form of malware designed to encrypt files rendering the files and systems unusable
- Incidents have become increasingly prevalent among government entities and critical infrastructure

- **Once encrypted, no security software or outside experts can restore the files**

Example of Ransomware Impact

Riviera Beach FLORIDA

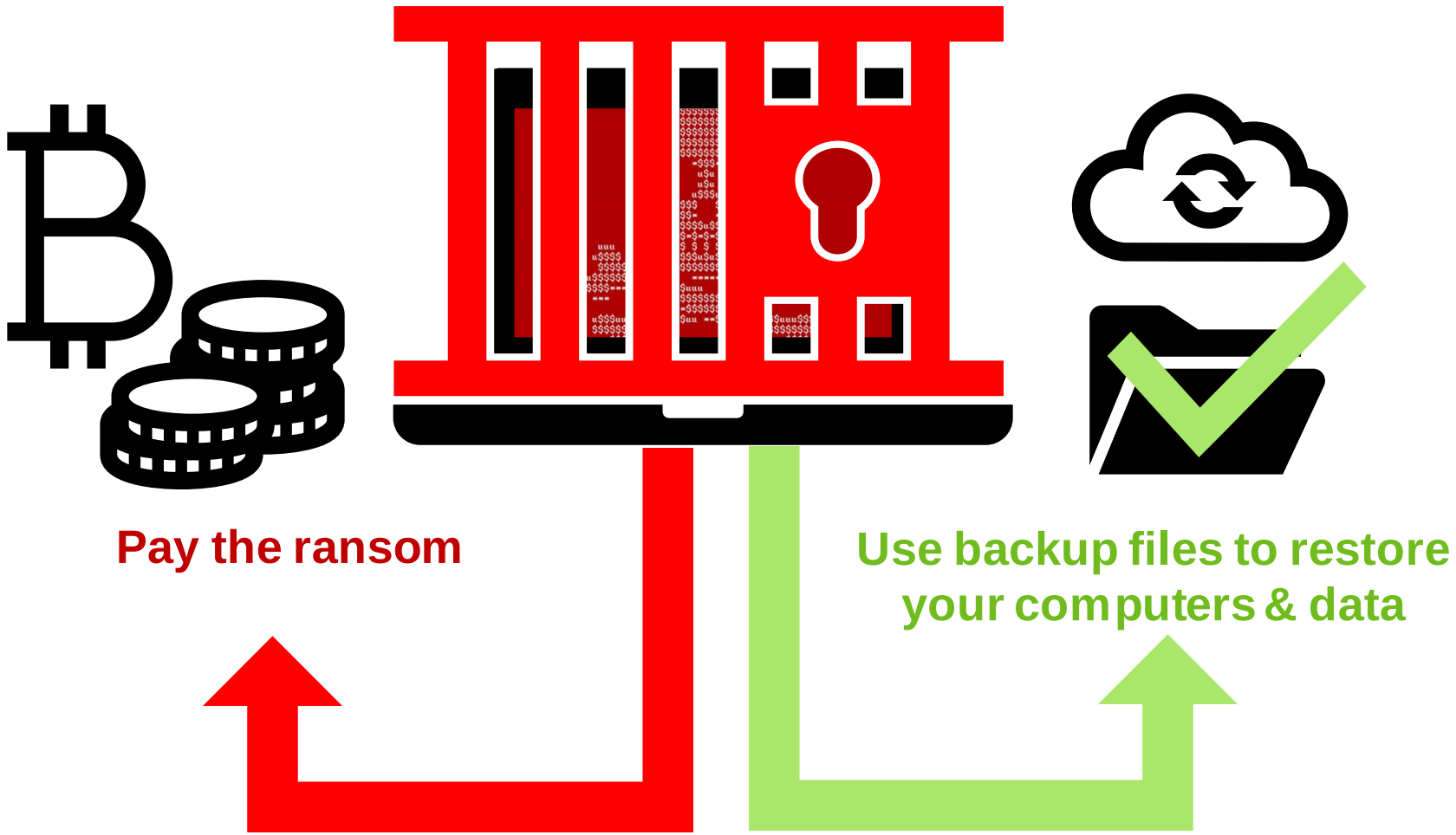
City with population of 32,000 paid ransom of over $600,000 and received the key to decrypt files.

6 Position PSAP

Phones, email, Public Works, City Attorney's office, Library - all municipal government systems were affected

…"CAD and Police Records were down for weeks.."

What Are Your Options?



If You Pay the Ransom...

- Payment does not guarantee the attacker will provide the encryption key

- According to "The State of Ransomware 2022" by Sophos, only 4% of organizations that paid got all their data back

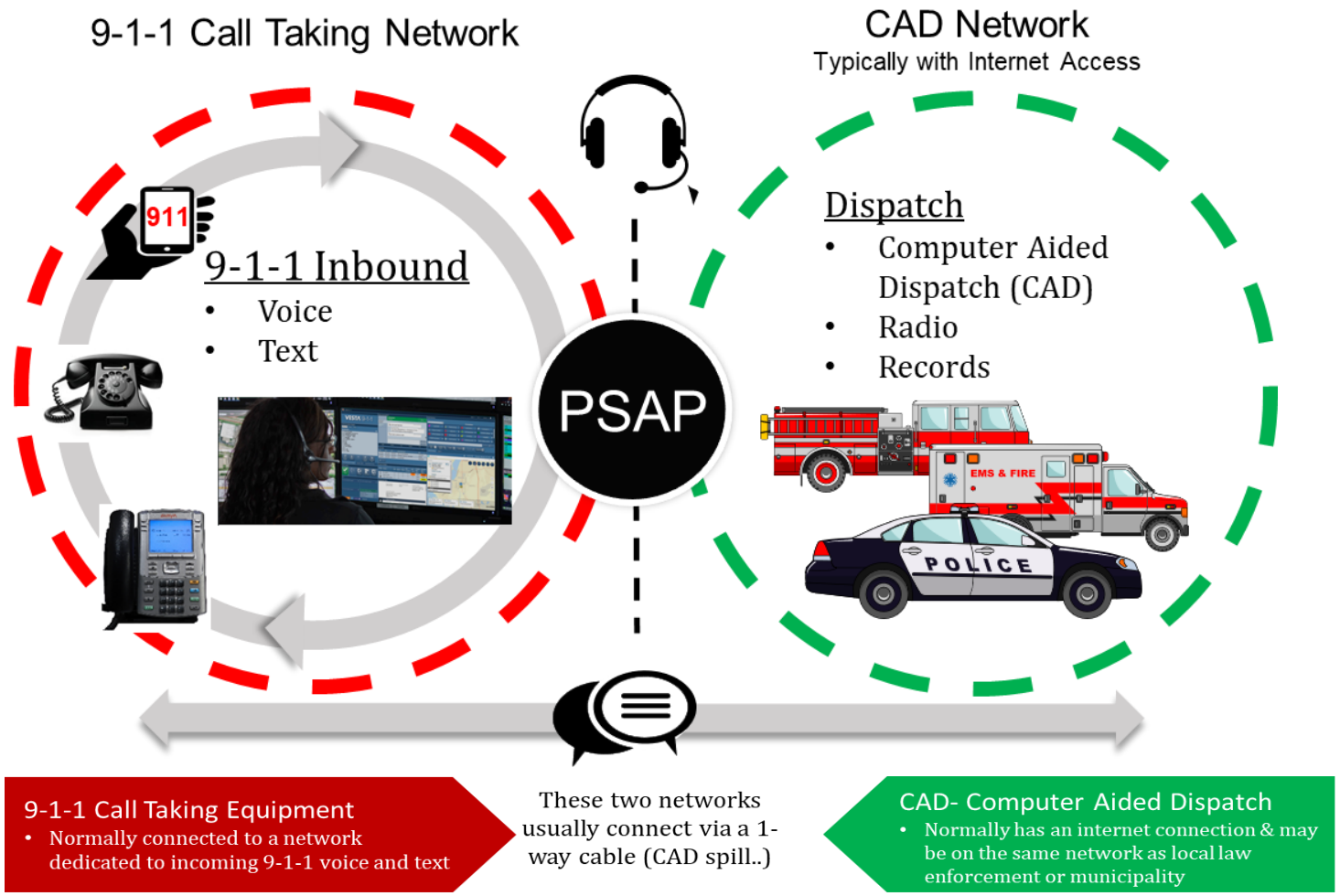
Best Practice – Current/Clean Backups

- Maintain them offline - having current backups is critical
- No need to pay a ransom for data that is readily accessible to your organization.
- Regularly scheduled
- Restoration Plan/Procedures in Place – Include your vendors

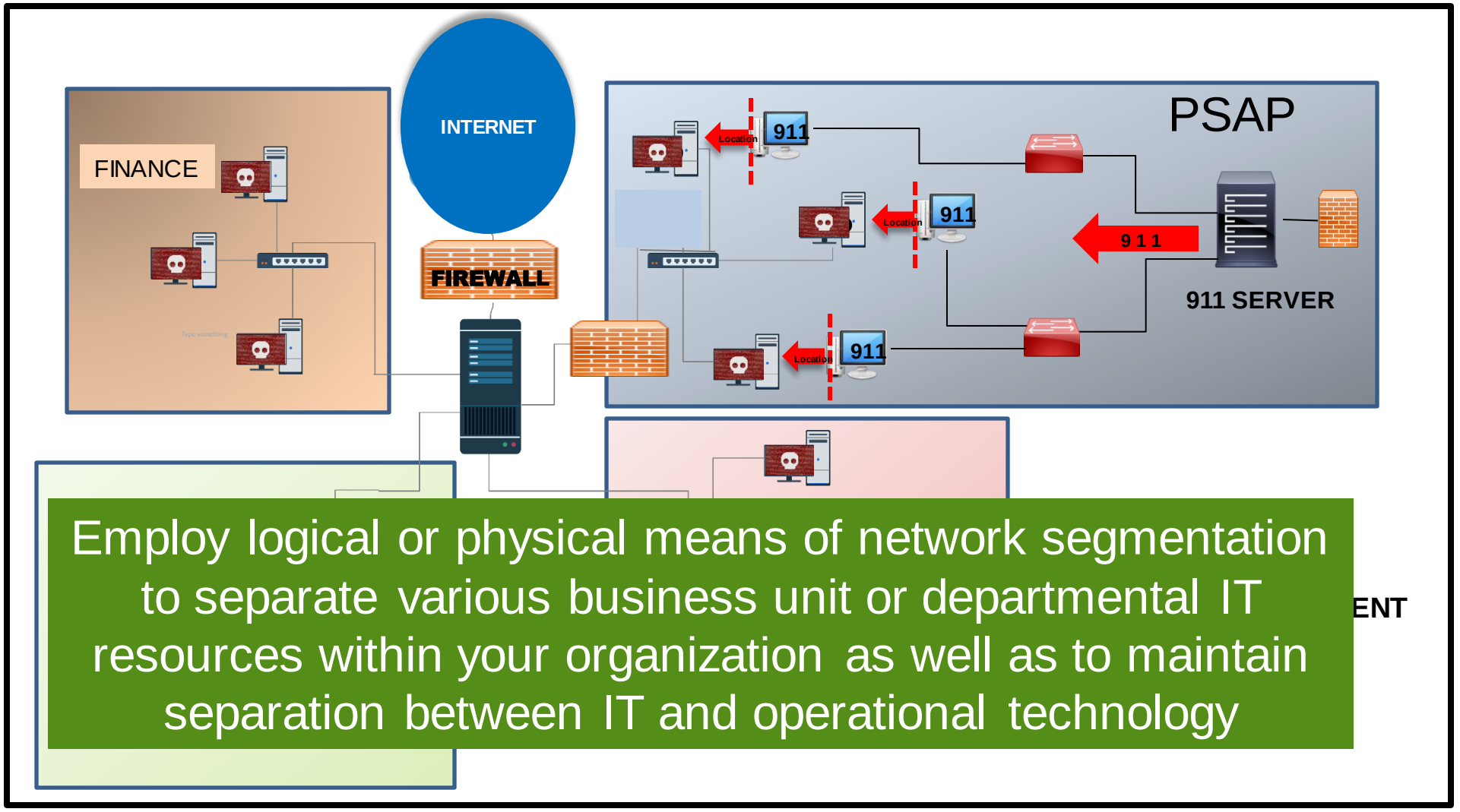
Lateral Attacks

- In the case of the Lateral Attack, the PSAP is an unintended target
- The cyberattack is on a different municipal department, but makes its way into all governmental systems, including the PSAP

PSAP – Dual Networks



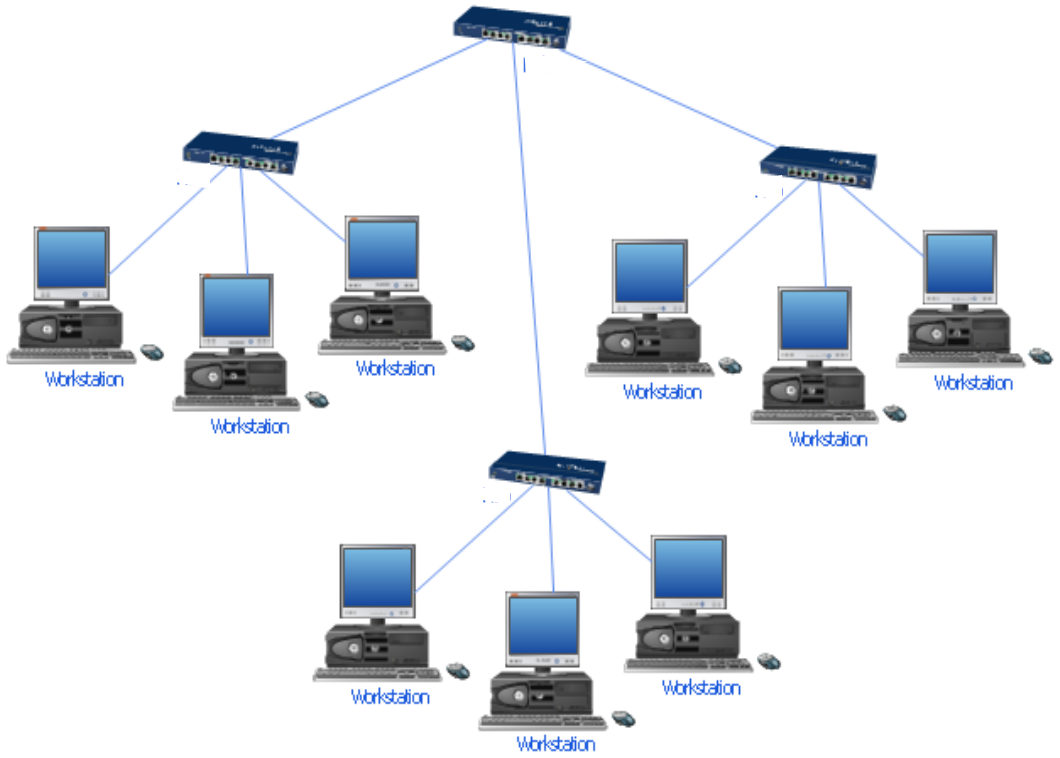
PSAP – Dual Networks



Employ logical or physical means of network segmentation to separate various business unit or departmental IT resources within your organization as well as to maintain separation between IT and operational technology

Best Practice – Segment LANs

- Vendors at some larger PSAPs are have started to place groups of workstations on separate LAN segments
- This model will help contain malware/ransomware or other negative events



Cryptojacking

- Mining crypto currency using your systems
- Goal is to stay undetected to maintain an ongoing revenue stream for the attacker

Cryptojacking is the Third Wave

- **1st Wave –** Hack into computer system, steal data and then sell it for profit (example credit card information)
- **2nd Wave –** Hack into computer system, lock it down with ransomware and demand payment in bitcoin
- **3rd Wave –** Hack into computer system and use the computing power, electricity and network access that someone else pays for to ‘mine’ cryptocurrencies for profit.

Detecting Cryptojacking

Slow performing CAD computers

Spike in electricity bill

Review outbound internet traffic

This happened to a PSAP in the Mid-Atlantic States

How Do They Get Into Your PSAP?

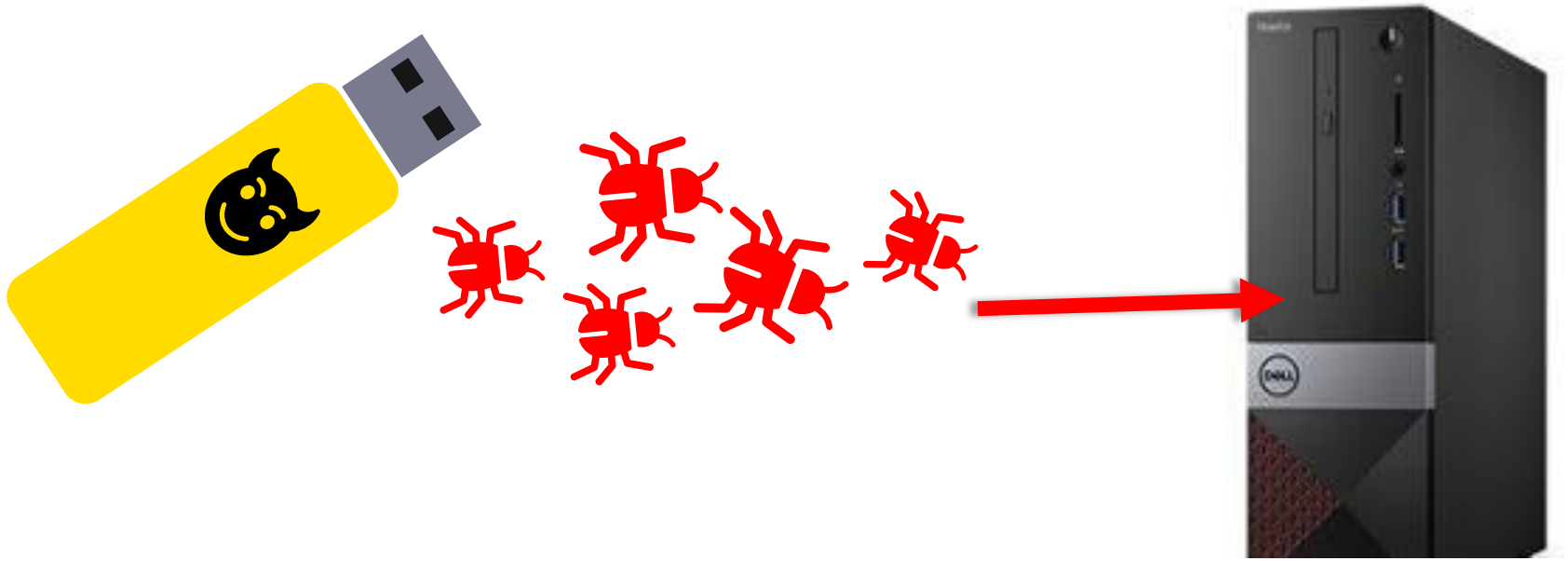
Most CAD systems have a web browser and internet connection on the workstation

www. .com

- **Phishing Attack:** Click on an attachment - File-based cryptojacking malware works just like regular malware. It loads directly onto a computer and runs quietly in the background.
- **Browser-based attacks:** Code is injected on websites or delivered with ads.
- **Insider:** Cases where an employee intentionally loads the cryptojacking malware on their employer's system

The Deadly USB Stick/Thumb Drive

- Thumb drives are the easiest way to transfer files between computers
- Also easy to transfer an infection behind the firewall

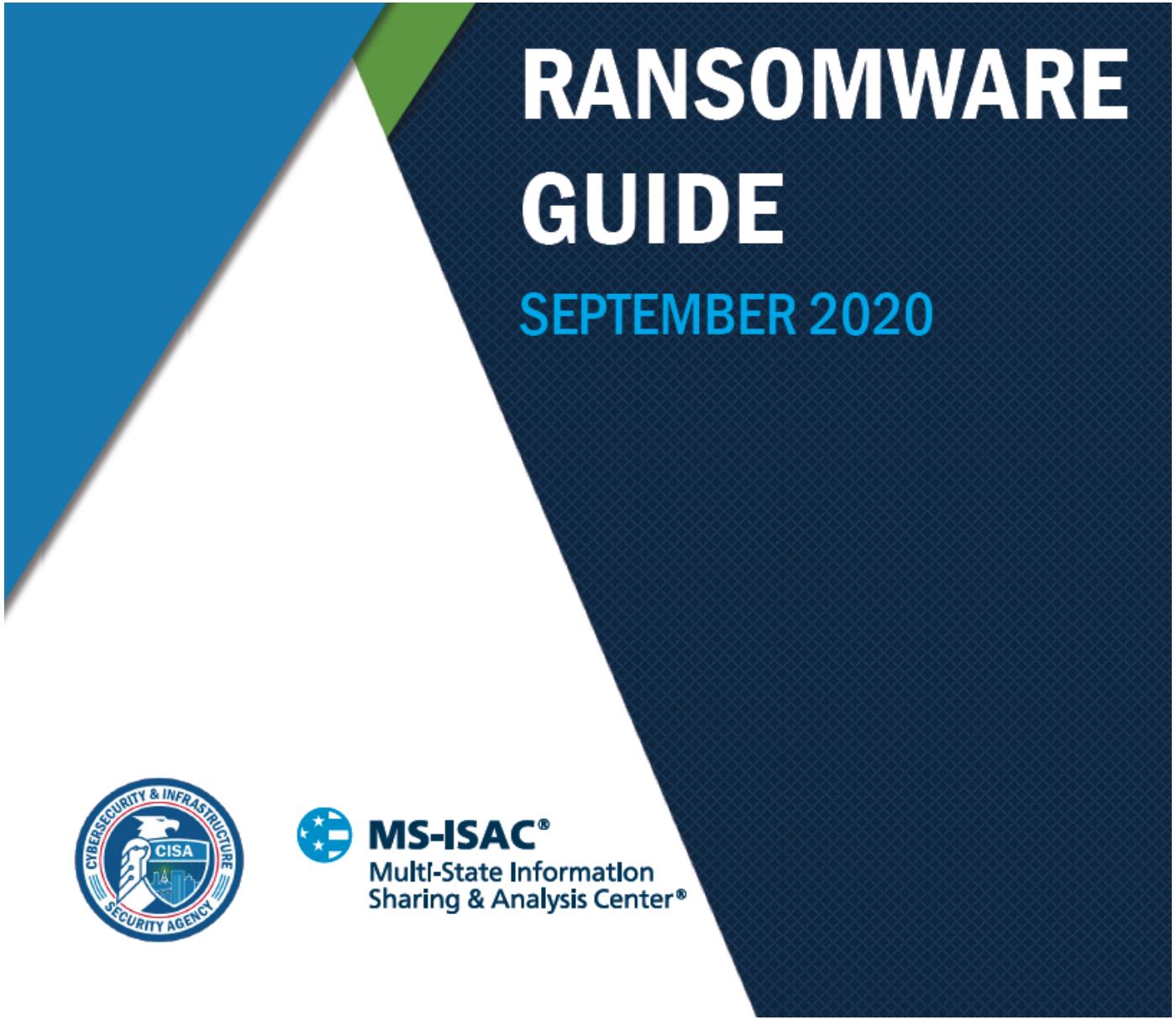


Best Practice – Do Not Allow Charging Smartphones via USB

It is recommended that personal smartphones not be allowed to be charged via a USB attached to any computer on the center's network

Best Practice – Disable USB Ports

- Disable USB Ports On PSAP Computers
- Access only available when an administrative password is entered


RANSOMWARE
GUIDE
SEPTEMBER 2020
MS-ISAC®
Multi-State Information
Sharing & Analysis Center®

Remote Access

- *Remote Access in General*
- *Working with Vendors*

Remote Access

- Even the most secure systems are made vulnerable when remote access is enabled
- Hackers are constantly trolling for systems with open access to attack

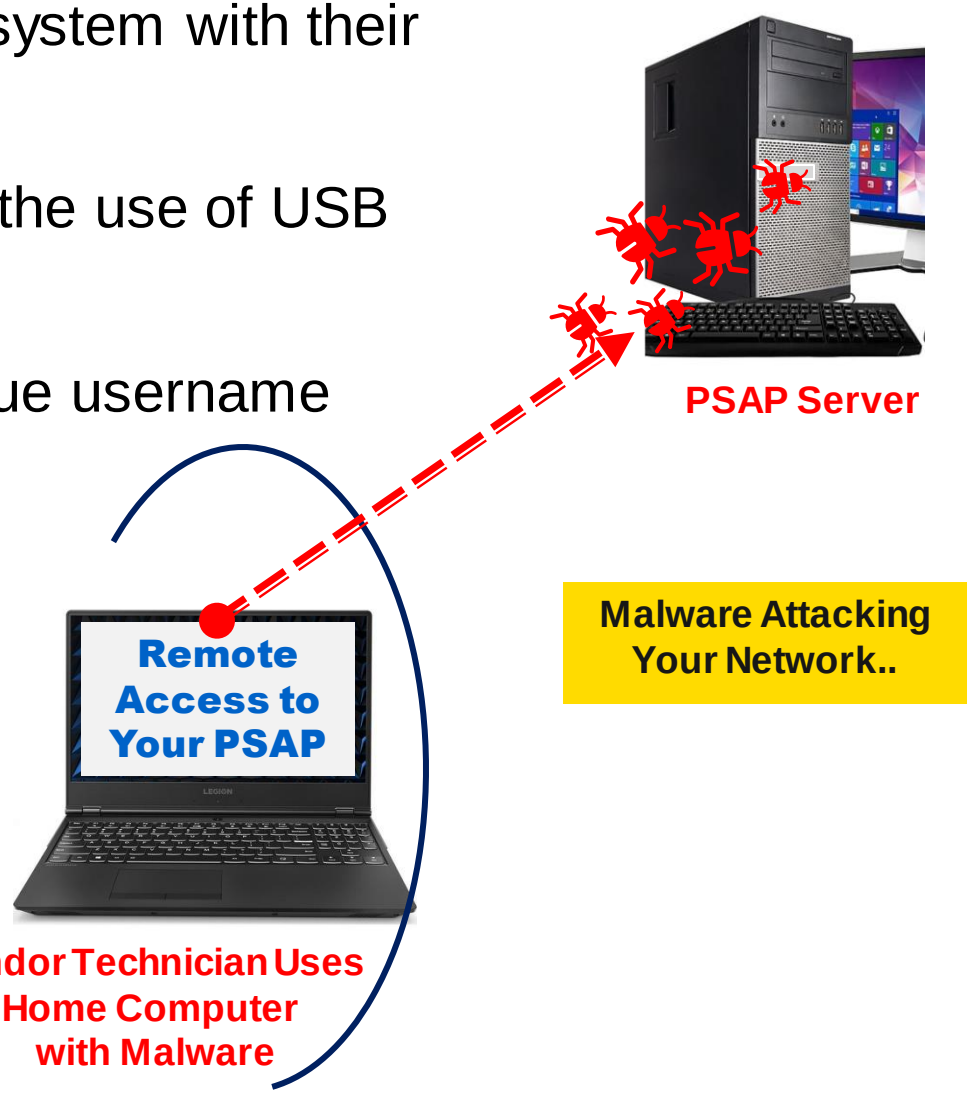
Any 'Closed Network' is made vulnerable by remote access

Working With Our Vendors – Risks

- Vendors provide valuable support, but also carry certain risks
- Take into consideration the risk management and cyber hygiene practices of third parties your organization relies on to meet its mission
- Vendors have been an infection point for ransomware

Your Vendors and Remote Access

- Can technicians remote into your system with their home computer?
- Does the vendor have policies for the use of USB drives?
- Does each technician have a unique username and password?



Best Practices - Remote Access

- Turn off Remote Access to your systems
- Only open it up when your vendor/support needs to access it
- Turn off Remote Access afterward

Best Practices – Your Vendor and Remote Access

- Vendors typically have remote access to your call handling system
- Request an audit of who has access to your system
- Insist that each person supporting your system has a unique login
- Ask your vendor how they handle accounts after an employee event (termination, resignation, promotion, etc.)

SECTION VI – CYBER HYGIENE & BEST PRACTICES

What is Cyber Hygiene?

- Practices and steps computer & device users can follow to maintain network health and online security

- Routines for computer & device use that improves the safety of personally identifiable information (PII) and other data that could be stolen or corrupted

Best Practice – Software Updates

Regularly update software as prompted, and/or update to current & better versions of software

Why Update?

- Patched security holes
- Improved functionality
- Bug Fixes

- We trust our vendors to keep our systems updated with the latest security patches…
- It is important to understand their policy for reviewing security alerts and installing updates
- Sooner rather than later!

Best Practice – Passwords

Use complex passwords that contain upper & lowercase, numbers and symbols

Ag3ofUlTr0n!
1NfiNityW@Rs%tH@N05

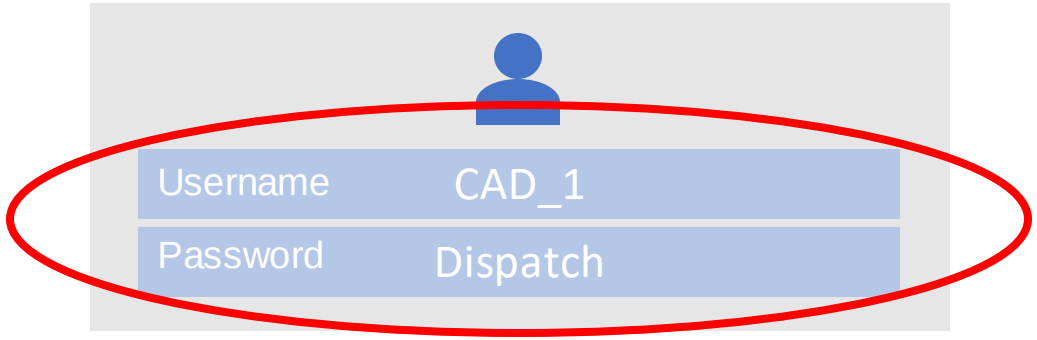
Regularly change passwords & NEVER post passwords where they are visible to other personnel, visitors, or could accidentally be seen in social media posts, etc.

Never send passwords over the internet, do not use the same password across logins & accounts

Strong Passwords

- Password Length: 8-16+
- Includes Symbols: @#%!$
- Includes Numbers: 123456…
- Includes Lowercase: abcdefg…
- Includes Uppercase: ABCDEFG

Best Practice – Individual Logons For All Users



- In numerous PSAPs across the country, all Telecommunicators use a single username and password for the 9-1-1 systems
- This provides no logging or auditing capability
- Your vendors may be using similar practice

Why This Area Is So Important?

- Username and passwords are the only things that keep the hackers out of your network
- Over 90% of successful attacks result from employee actions like clicking on an infected item/link
- People are not as good at identifying a potential attack as they think they are

Credentials – Outsiders

Multi-Factor Authentication should go beyond our own people

Mutual Aid:

- If we bring in personnel from other PSAPs and public safety entities through mutual aid, what are our SOPs for credentialing these end-users & what permissions do they have on our systems?

Vendors:

- If we have vendors accessing our systems, secure physical areas, etc. for maintenance or incident response, what are our SOPs for credentialing and verifying these end-users or technicians?

Best Practices and CISA Guidance (1 of 5)

- Review the sender's email address carefully – It could it be “spoofed”
- Watch for mistakes in spelling and grammar
- Phishing emails usually use non-personalized greetings
- Do not act if you feel pressured: phishers usually create a sense of urgency

Best Practices and CISA Guidance (2 of 5)

- Watch out for file extensions in attachments. File.docx.exe or File.pdf.exe are executable programs that may harm your computer
- Double-check any links by hovering over them
- If a site claims to be an official government publication, check the URL to see if it ends in .gov

Best Practices and CISA Guidance (3 of 5)

- Recent Windows vulnerabilities continue to be exploited – download updates automatically and install them
- Phishing emails hijacking the user's system through MS-Office 365 have risen dramatically – Includes 3rd Party Outlook Add-Ins
- If you already opened an MS Office that is asking you to "Enable Content", close and delete that document immediately

Best Practices and CISA Guidance (4 of 5)

- Be leery when asked for info that you are not used to being asked for
- Avoid clicking on links in unsolicited emails
- Do not respond to email solicitations for personal information
- If in doubt, use out of band verification via phone, SMS or chat

Best Practices and CISA Guidance (5 of 5)

- Turn off your email client's option to automatically download attachments
- Use trusted sources—such as legitimate, government websites for up-to-date, fact-based information about COVID-19

SECTION VII – RESPONDING TO AND REPORTING CYBER INCIDENTS

It's Almost Inevitable...

- It's no longer a question of if your systems will be successfully attacked, it's just a question of when...
- Must have some plans in place to minimize the impact

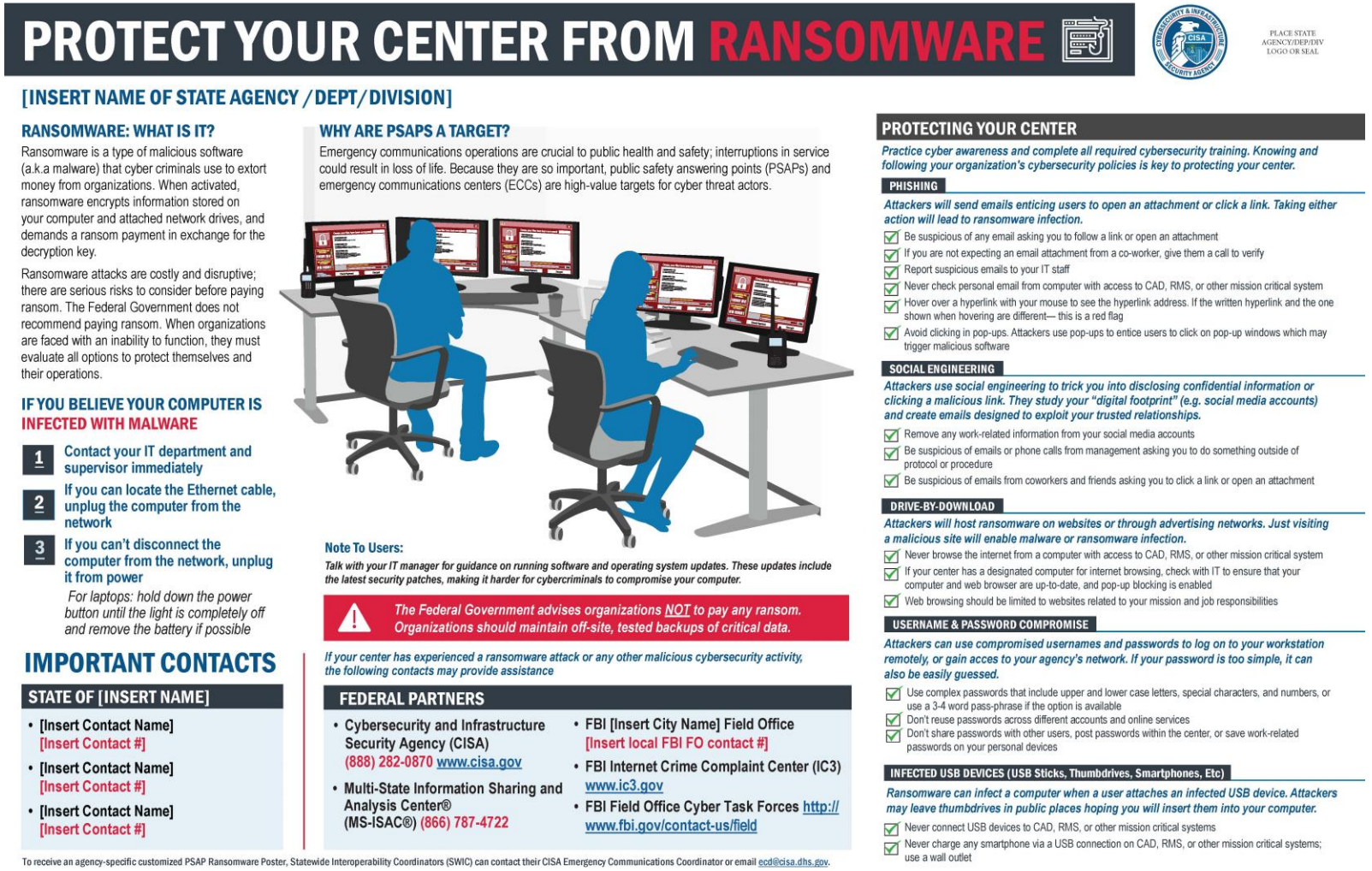
CAD Is Down – What Can We Do?

- Need to be able to continue to operate, dispatch units, document activities, etc.
- Establish an Essential Records Program
  - Records necessary to the continuing essential functions and resumption of normal operations
  - Run Cards/Unit Recommendations
  - Documentation of critical information items
- Incorporate Essential Records Program into overall continuity plans

www.dhs.gov/emergency-services-sector-continuity-planning-suite

Building Awareness

CISA poster program



PROTECT YOUR CENTER FROM RANSOMWARE

PLACE STATE AGENCY/DEPT/DIV LOGO OR SEAL

[INSERT NAME OF STATE AGENCY / DEPT / DIVISION]

RANSOMWARE: WHAT IS IT?

Ransomware is a type of malicious software (a.k.a malware) that cyber criminals use to extort money from organizations. When activated, ransomware encrypts information stored on your computer and attached network drives, and demands a ransom payment in exchange for the decryption key.

Ransomware attacks are costly and disruptive; there are serious risks to consider before paying ransom. The Federal Government does not recommend paying ransom. When organizations are faced with an inability to function, they must evaluate all options to protect themselves and their operations.

IF YOU BELIEVE YOUR COMPUTER IS INFECTED WITH MALWARE

1. Contact your IT department and supervisor immediately
2. If you can locate the Ethernet cable, unplug the computer from the network
3. If you can't disconnect the computer from the network, unplug it from power

For laptops: hold down the power button until the light is completely off and remove the battery if possible

WHY ARE PSAPS A TARGET?

Emergency communications operations are crucial to public health and safety; interruptions in service could result in loss of life. Because they are so important, public safety answering points (PSAPs) and emergency communications centers (ECCs) are high-value targets for cyber threat actors.

Note To Users:

Talk with your IT manager for guidance on running software and operating system updates. These updates include the latest security patches, making it harder for cybercriminals to compromise your computer.

The Federal Government advises organizations NOT to pay any ransom. Organizations should maintain off-site, tested backups of critical data.

IMPORTANT CONTACTS

If your center has experienced a ransomware attack or any other malicious cybersecurity activity, the following contacts may provide assistance

STATE OF [INSERT NAME]

- [Insert Contact Name] [Insert Contact #]
- [Insert Contact Name] [Insert Contact #]
- [Insert Contact Name] [Insert Contact #]

FEDERAL PARTNERS

- Cybersecurity and Infrastructure Security Agency (CISA) (888) 282-0870 www.cisa.gov
- Multi-State Information Sharing and Analysis Center® (MS-ISAC®) (866) 787-4722
- FBI [Insert City Name] Field Office [Insert local FBI FO contact #]
- FBI Internet Crime Complaint Center (IC3) www.ic3.gov
- FBI Field Office Cyber Task Forces http://www.fbi.gov/contact-us/field

To receive an agency-specific customized PSAP Ransomware Poster, Statewide Interoperability Coordinators (SWIC) can contact their CISA Emergency Communications Coordinator or email ecd@cisa.dhs.gov.

PROTECTING YOUR CENTER

Practice cyber awareness and complete all required cybersecurity training. Knowing and following your organization's cybersecurity policies is key to protecting your center.

PHISHING

Attackers will send emails enticing users to open an attachment or click a link. Taking either action will lead to ransomware infection.

- ☑ Be suspicious of any email asking you to follow a link or open an attachment
- ☑ If you are not expecting an email attachment from a co-worker, give them a call to verify
- ☑ Report suspicious emails to your IT staff
- ☑ Never check personal email from computer with access to CAD, RMS, or other mission critical system
- ☑ Hover over a hyperlink with your mouse to see the hyperlink address. If the written hyperlink and the one shown when hovering are different— this is a red flag
- ☑ Avoid clicking in pop-ups. Attackers use pop-ups to entice users to click on pop-up windows which may trigger malicious software

SOCIAL ENGINEERING

Attackers use social engineering to trick you into disclosing confidential information or clicking a malicious link. They study your "digital footprint" (e.g. social media accounts) and create emails designed to exploit your trusted relationships.

- ☑ Remove any work-related information from your social media accounts
- ☑ Be suspicious of emails or phone calls from management asking you to do something outside of protocol or procedure
- ☑ Be suspicious of emails from coworkers and friends asking you to click a link or open an attachment

DRIVE-BY-DOWNLOAD

Attackers will host ransomware on websites or through advertising networks. Just visiting a malicious site will enable malware or ransomware infection.

- ☑ Never browse the internet from a computer with access to CAD, RMS, or other mission critical system
- ☑ If your center has a designated computer for internet browsing, check with IT to ensure that your computer and web browser are up-to-date, and pop-up blocking is enabled
- ☑ Web browsing should be limited to websites related to your mission and job responsibilities

USERNAME & PASSWORD COMPROMISE

Attackers can use compromised usernames and passwords to log on to your workstation remotely, or gain acces to your agency's network. If your password is too simple, it can also be easily guessed.

- ☑ Use complex passwords that include upper and lower case letters, special characters, and numbers, or use a 3-4 word pass-phrase if the option is available
- ☑ Don't reuse passwords across different accounts and online services
- ☑ Don't share passwords with other users, post passwords within the center, or save work-related passwords on your personal devices

INFECTED USB DEVICES (USB Sticks, Thumbdrives, Smartphones, Etc)

Ransomware can infect a computer when a user attaches an infected USB device. Attackers may leave thumbdrives in public places hoping you will insert them into your computer.

- ☑ Never connect USB devices to CAD, RMS, or other mission critical systems
- ☑ Never charge any smartphone via a USB connection on CAD, RMS, or other mission critical systems; use a wall outlet

Cyber Incident Response Plan

Contact Information

Consider filling out the following contact information for ready use should your organization become a victim of a ransomware incident. Consider contacting these organizations for mitigation and response assistance or for purpose of notification.

State and Local Response Contacts:		
Contact	**24x7 Contact Information**	**Roles and Responsibilities**
IT/IT Security Team - Centralized Cyber Incident Reporting		
Departmental or Elected Leaders		
State and Local Law Enforcement		
Fusion Center		
Managed/Security Service Providers		
Cyber Insurance		

Ransomware Quick References

- **Ransomware – Guidance & Resources (CISA)** www.cisa.gov/ransomware
- Resources For State, Local and Tribal Governments (CISA)
  - Case Studies
  - Toolkits
  - https://us-cert.cisa.gov/resources/sltt

Basic Response Planning Includes

1. Emergency contact list
2. Immediate actions to take
3. Notifications that need to be made
4. Develop an essential procedures and documents package so you can continue to function
5. Verify the existence and cleanliness of offline backups
6. Restoration procedures and resources
7. Forensic analysis/after-action report

Government Resources

- **CISA Provides**
  - Risk Assessments – Next slide
  - Cyber Exercises – To evaluate or help develop your cyber incident response plan
  - Cybersecurity Advisors (CSAs) - Advise on best practices and connect you to resources to manage cyber risk
- **DHS/ECD Resources**
  - Various resources are available in the areas of technology, sustainment, resilience, etc. are available
- **See Supplemental Handout for list an hotlinks**

SECTION VIII – SUMMARY

The Bottom Line…

- **PSAPs/ECCs Are Direct/Indirect Targets**
- **Attacks**
  - Are inevitable and will cause disruption
  - Some attacks hit behind the firewall
  - Admin/records and/or 9-1-1
  - Workarounds may help
- **TDoS Is A Real Threat**
  - Appliances may help
  - FCC will not block them

The Bottom Line…

- **Ransomware Can Cause Weeks of Downtime**
  - Segmented LANs will limit disruption
  - Offline/clean/current backups are critical
  - Have an Essential Records Program to allow continuity of operations during downtime (pen and paper/forms)
- **Employee Actions**
  - Disable USB ports/admin password access only
  - No social media or web-based personal email

The Bottom Line…

- **Vendors**
  - Critical, but there are risks with remote access
  - Require unique usernames/passwords for all users
  - Request policies and review them
  - Verify that the backups they generate will be “clean”
- **Phishing Is The Biggest Threat**
  - The key is employee education & training on a regular basis
  - COVID-19 increases vulnerability

The Bottom Line…

- **Phishing (continued)**
  - Social Engineering is how they get people to “bite”
  - Practice what you preach
  - Senior management is often the most vulnerable
- **Other Best Practices**
  - Individual logons for everyone
  - Install all software updates on a timely basis
  - Protect or limit access to physical assets, especially those outside of the dispatch center

The Bottom Line…

- **Responding To/Reporting Cyber Incidents**
  - It's not "if", it's a question of "when"
  - Need to be prepared
  - Develop and exercise a plan
  - Must have clean/offline backups to restore
  - Involve your vendors
  - See links for FBI, DHS, etc. contacts
  - Document actions for reference and/or insurance purposes

SECTION IX – CLOSING COMMENTS

Closing Comments (1 of 3)

- The focus of this program was awareness
- Hopefully, it expended your understanding of cybersecurity threats that are faced by PSAPs and ECCs on a daily basis
- Remember that even our radios are now computers

Closing Comments (2 of 3)

- Just because you don't know of any attacks on your systems doesn't mean they aren't happening
- It is important that you have some type of plan to address the inevitability of your system(s) going down at some point
- Consider implementing some of the policies, procedures, actions and controls included in this webinar to protect your systems

Closing Comments (3 of 3)

- We hope that you found this program interesting and worthwhile
- Consider the full day cybersecurity program and/or a full site assessment
- Thank you for your time and attention
- Questions?

Registering Your Attendance

- Please send an email to the following people to confirm your attendance:

darinanderson@nd.gov

awhite@lafayettegroup.com (if you want the handouts after the session)


CYBERSECURITY & INFRASTRUCTURE
CISA
SECURITY AGENCY