PSAP CYBERSECURITY AWARENESS WEBINAR

WEST VIRGINIA

Agenda

Cybersecurity and Threats to PSAPs

- Introductions & Overview
- Cybersecurity Threats to PSAPs & ECCs
- USB Port Awareness
- Social Media
- Working with Vendors
- Cyber Hygiene & Best Practices Next Steps
- Next Steps & Concluding Comments

PSAP & ECC Cybersecurity

Defending:

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

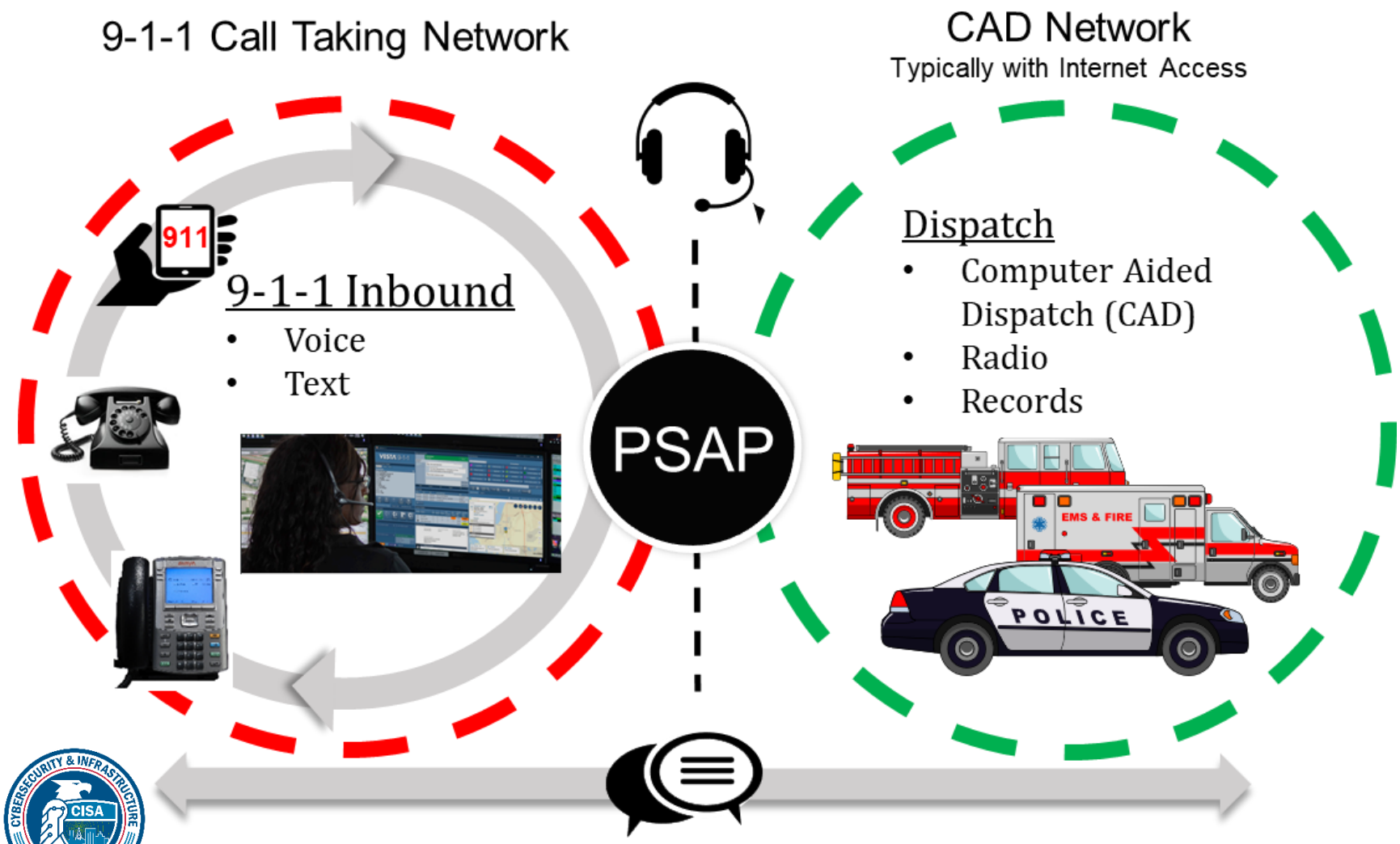
CYBERSECURITY THREATS TO PSAPS & ECCS

PSAP/ECC as a Target

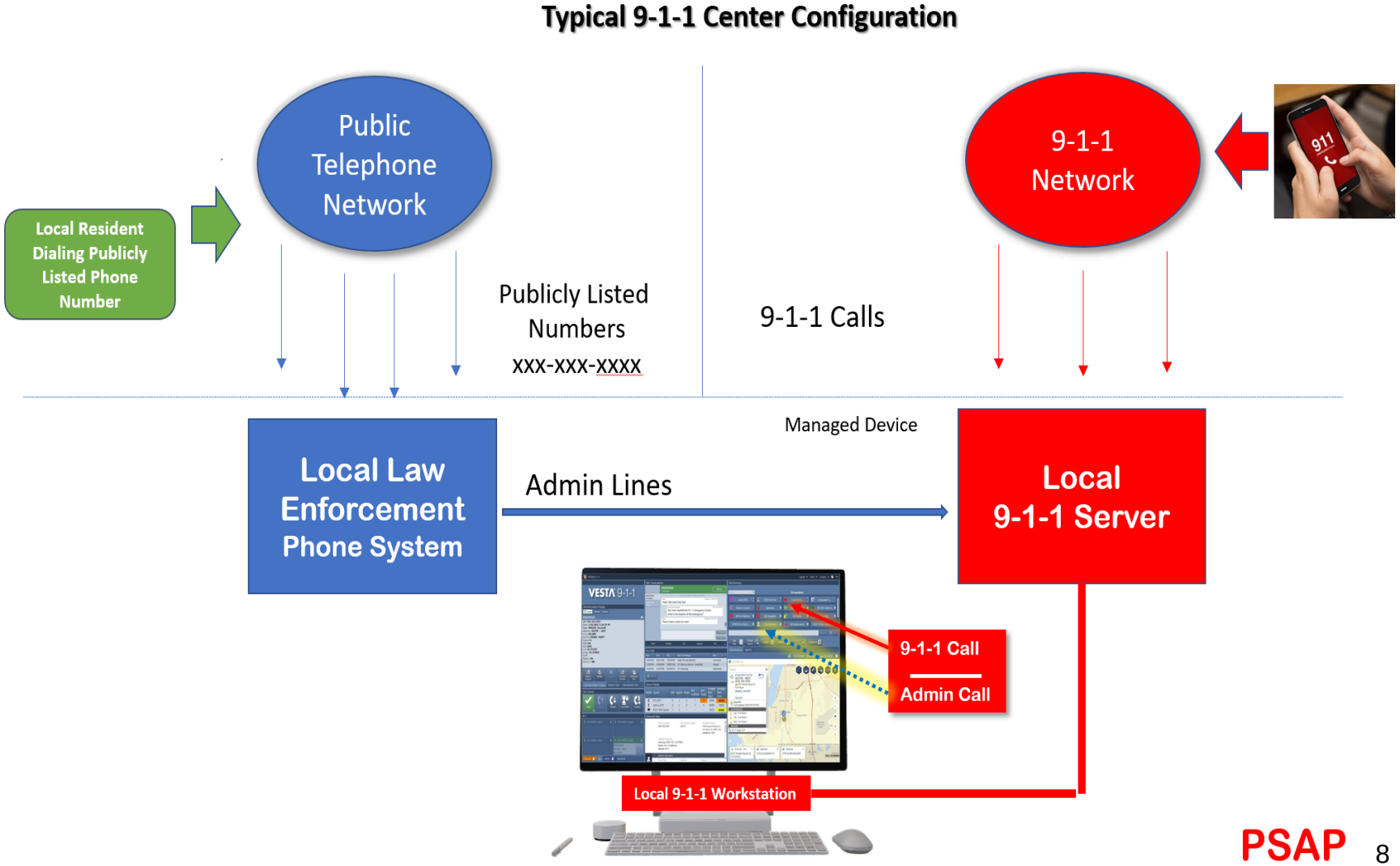
- **Disruption -** Cyber Attacks may shut down public access to 9-1-1, leading to public confusion and disrupting the dispatch of First Responders
- **Ransom -** As the networks, data and services are vital to public safety, PSAPs are more likely to pay a Bitcoin ransom in order to restore service
-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

TELEPHONY DENIAL OF SERVICE (TDoS)

PSAP – Dual Networks



Typical PSAP Configuration



Cyber Attacks (TDoS) Actors

- 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

Telephony Denial of Service

HACKED CONFERENCE BRIDGE

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

Industry Best Practice-TDoS Appliance

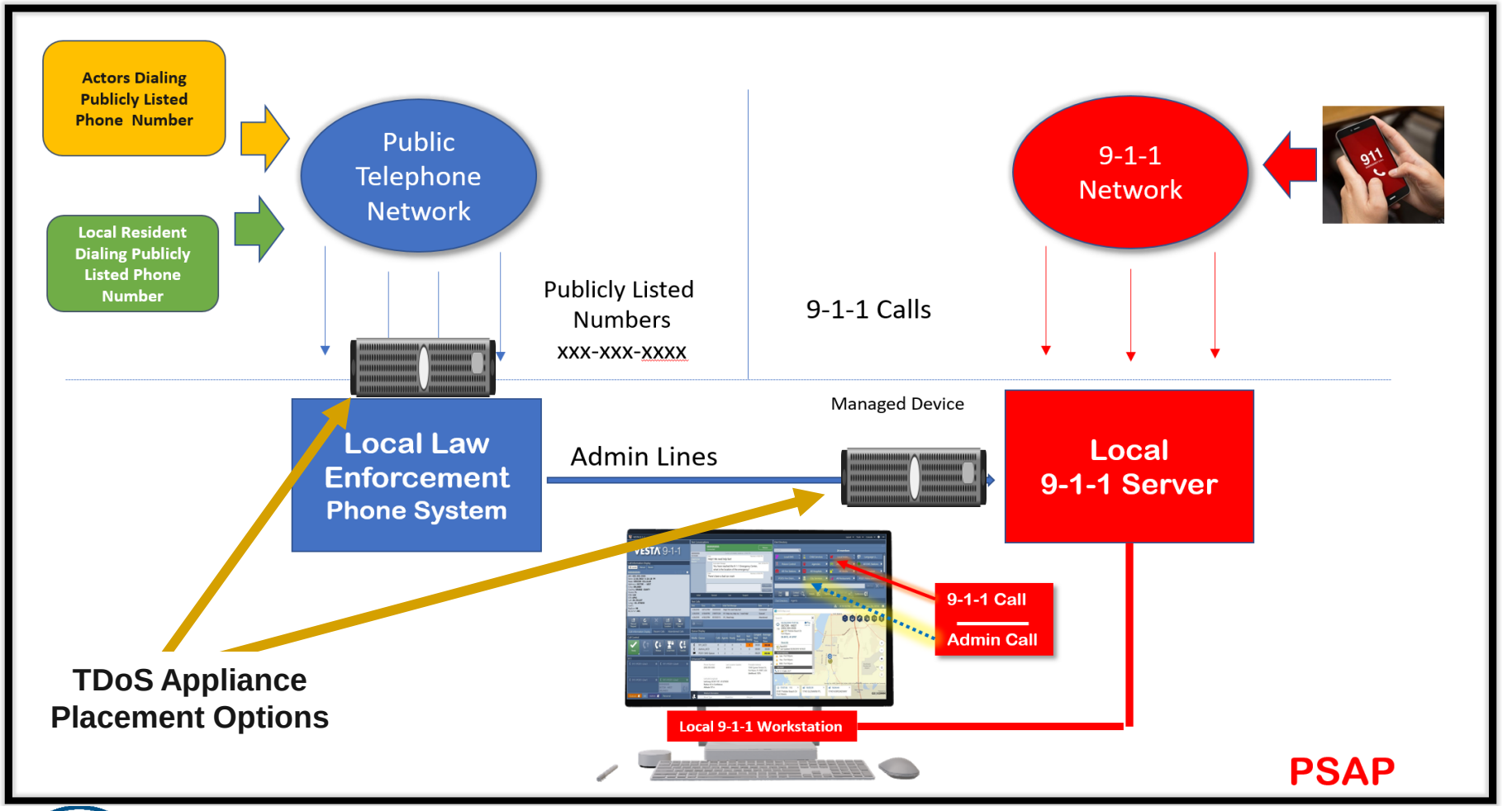
Industry Examples

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

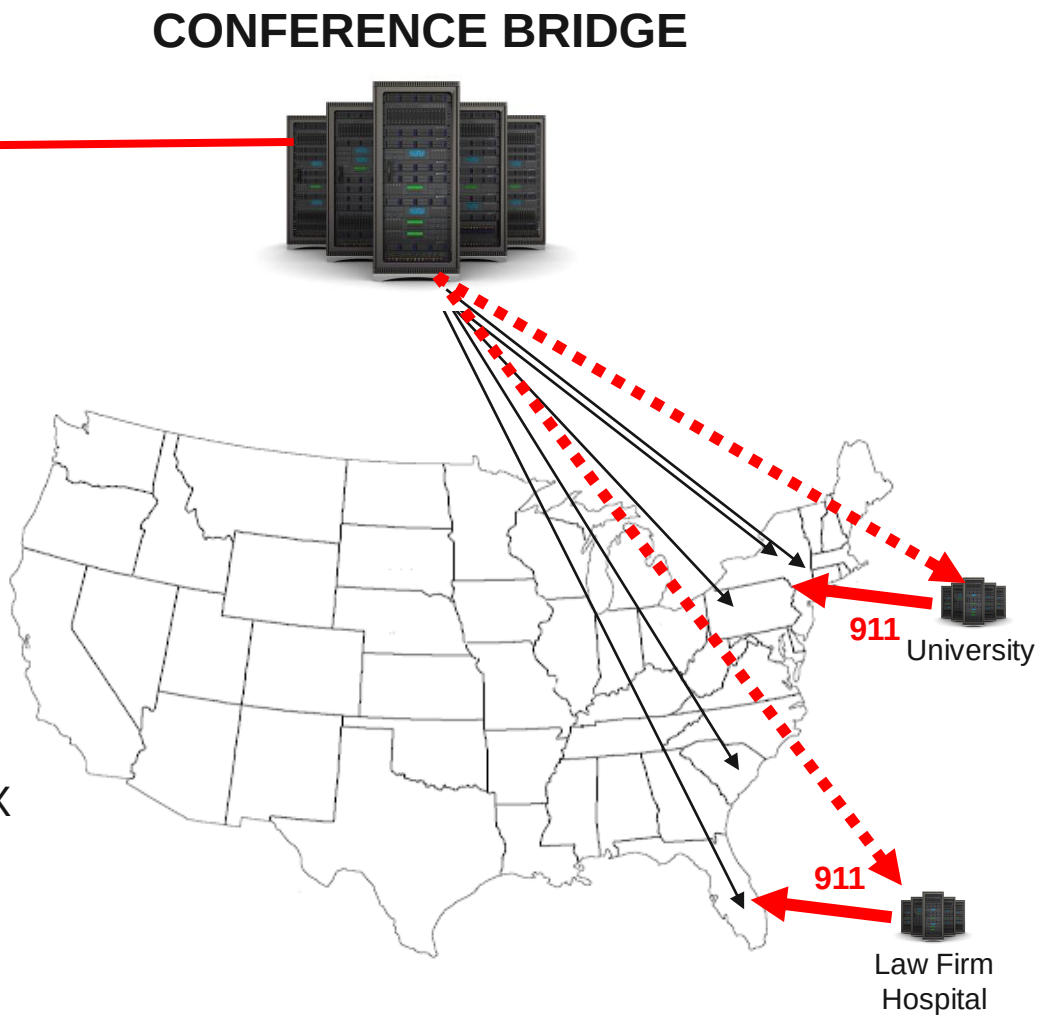
Recommendations

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

Protecting Admin Lines



Telephony Denial of Service - 911
Recent Attack Scenario in Numerous States



1. Select municipal target
2. Hunt for a PBX to Hack
3. Configure the PBX to call 9-1-1 repeatedly
4. In some cases, conference 911 PBX attack with admin line attack

9-1-1 During a TDoS Attack

If your Center gets attacked, you should be prepared to:

- Dispatch Law Enforcement to the Address
- Contact Your Carrier to Request Assistance
- Contact Any Center that handles your rollover

“Cyber Reflection” – What Does This Mean?

- 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?

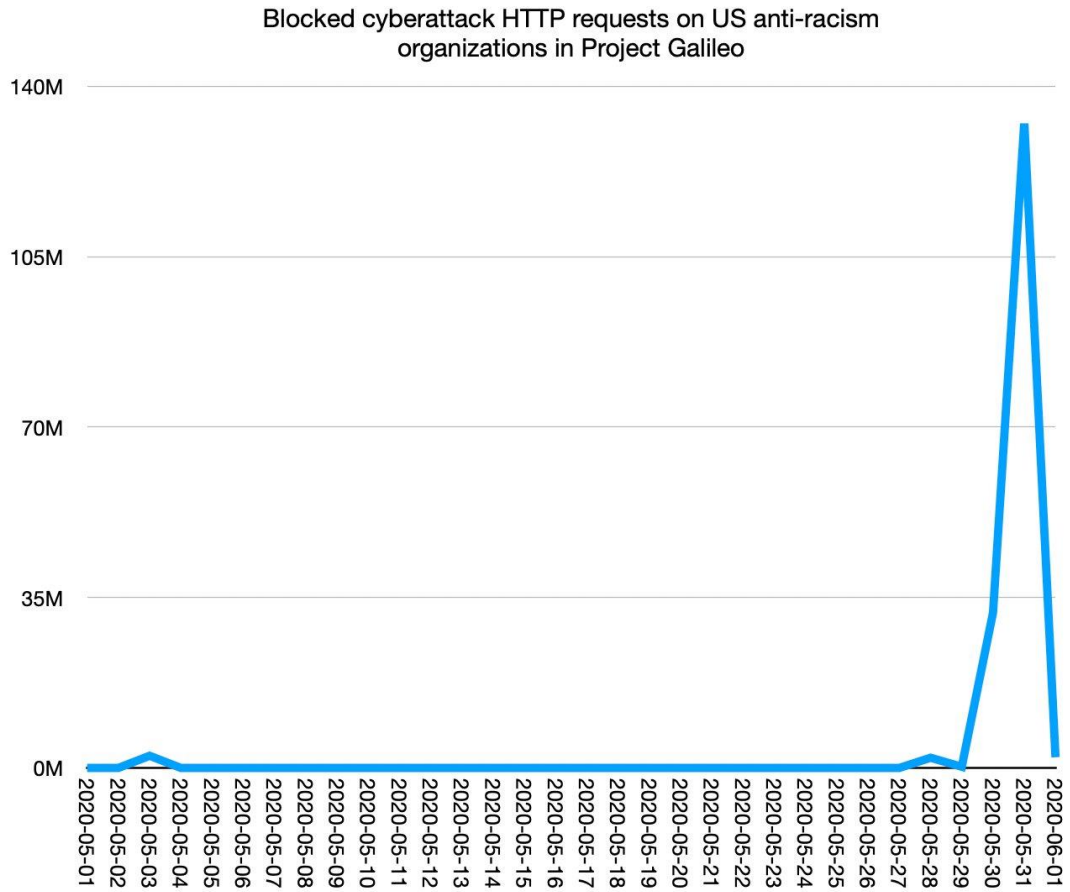
- **Disruption –** Cyberattacks may shut down public access to 9-1-1, leading to public confusion and disrupting dispatch
- **Disinformation** – Spreading false or misleading information about the events or situation
- **Loss of Confidence** – If citizens are unable to connect with law enforcement/PSAP,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

Cyberattacks During Civil Unrest – 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

Cyberattacks During Civil Unrest – How?

- Primary Type of Attack = DDoS



Cyberattacks During Civil Unrest – CISA Recommendations

- Enroll in a DoS protection service that detects abnormal traffic flows and redirects traffic away from your network
- Create a disaster recovery plan to ensure successful and efficient communication, mitigation, and recovery in the event of an attack
- Install and maintain antivirus software
- Install a firewall and configure it to restrict traffic coming into and leaving your computer
- Evaluate security settings and follow good security practices in order to minimalize the access other people have to your information

RANSOMWARE

Ransomware

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

- A form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable.
- Incidents have become increasingly prevalent among the Nation's state, local, tribal, and territorial (SLTT) government entities and critical infrastructure
- Once cybercriminals have encrypted your files, no security software or outside experts can restore them

Example of Ransomware Impact

Riviera Beach
FLORIDA

May 2019

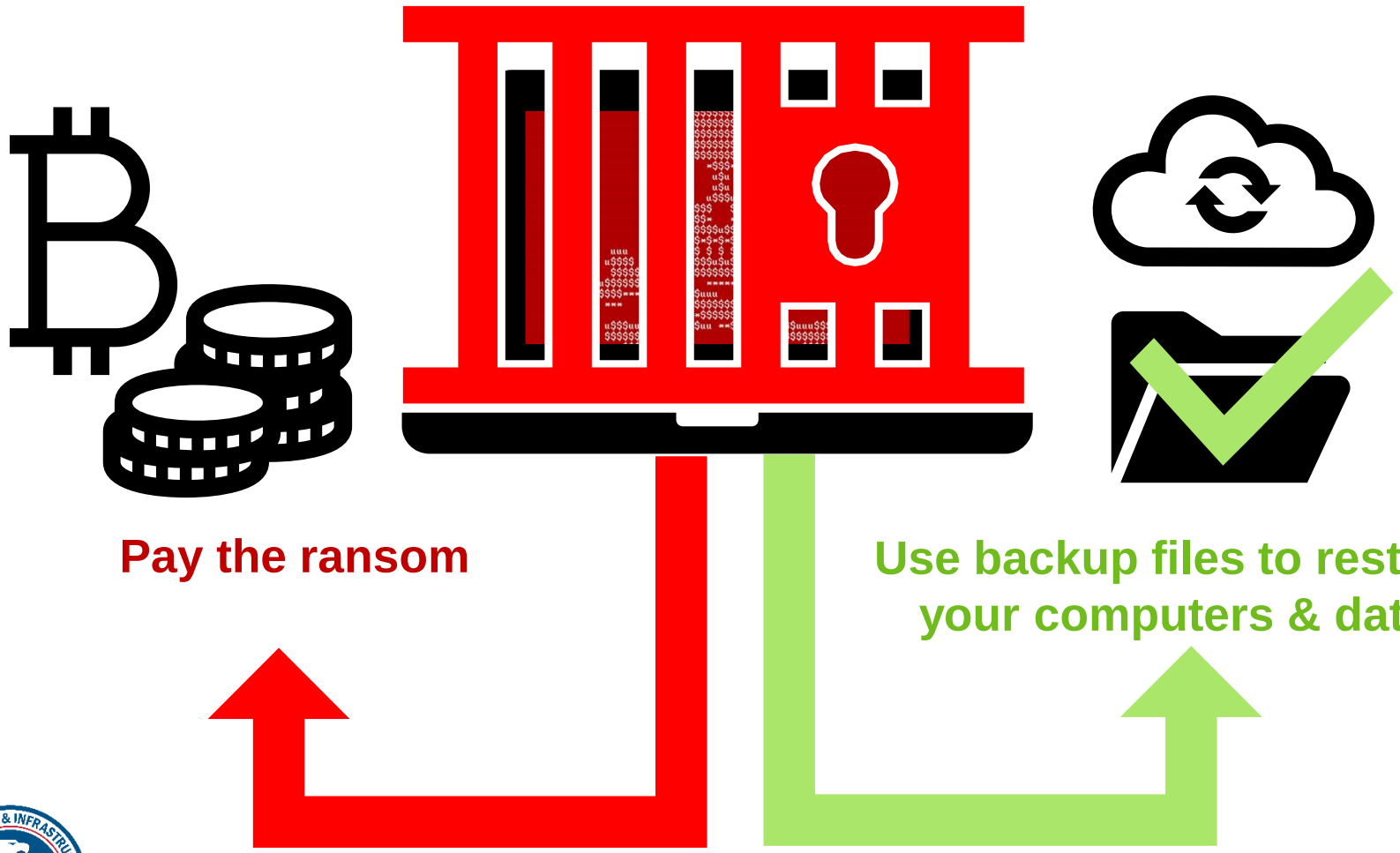
City with population of 32,000 paid ransom of over $600,000 and received the key to decrypt files.

6 Position PSAP

Phones, email, Public Works, City Attorneys office, Library - all municipal government systems were affected

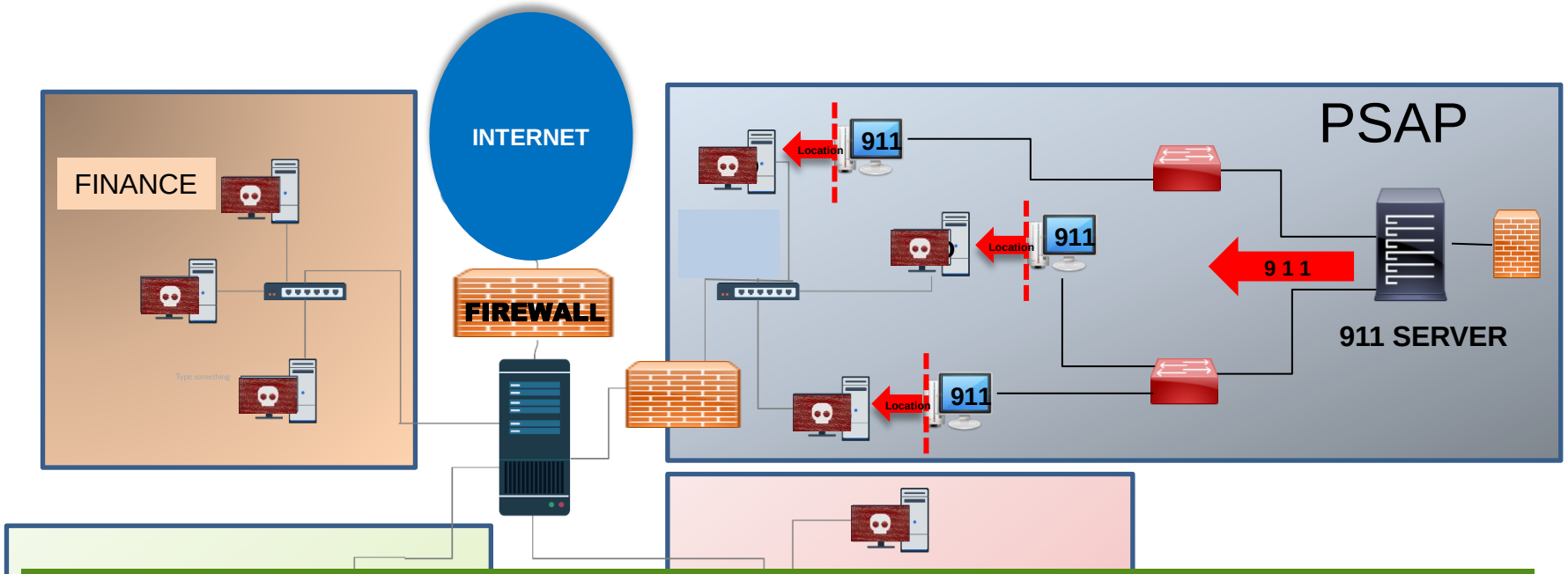
…"CAD and Police Records were down for weeks.."

What Are Your Options?



LATERAL ATTACKS

Ransomware Scenario (PSAP Example)



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

CAD Is Down – What Can We Do?

- First, make sure that 9-1-1 is still operational – If not, need to get back-up or transfer PSAP site activated
- Next, need to notify your PSAP/ECC manager
- We need to be able to continue to operate, dispatch units, document activities, etc.
- There should be a back-up plan

What's The Back-Up Plan?

- **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**

PHYSICAL SECURITY

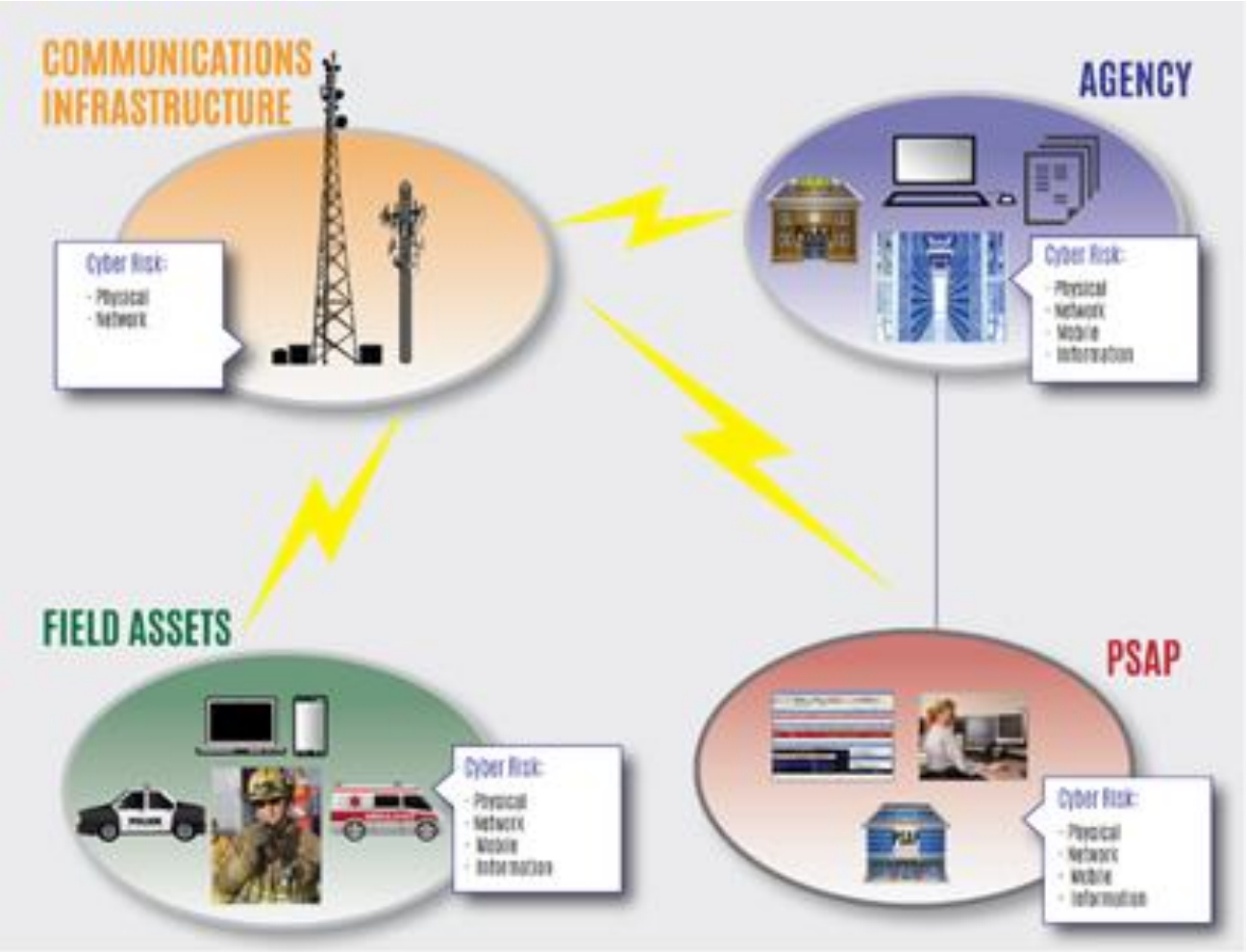
Need To Secure Physical Assets

- Not just the dispatch room/center
- Where are the main components and who has access to them?
- Do vendors and others have access?

Outside Of The PSAP/ECC Facility

- Any asset that is connected to the network can be attacked
- Keep an inventory of those assets
- How are the assets outside of the dispatch center protected?
  - MDTs & iPads
  - Network & antenna sites

What Assets Are At Risk?



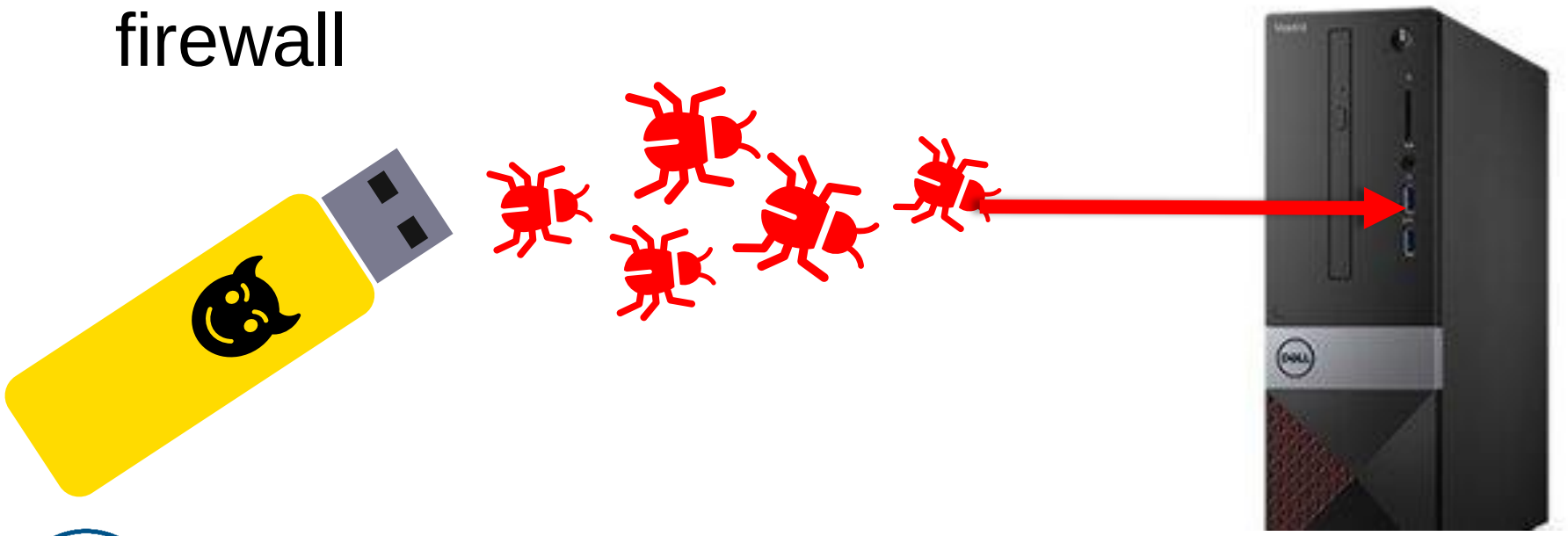
Need To Monitor Asset Status

- Any asset that is connected to the network can be attacked
- Keep an inventory of those assets
- How are the assets outside of the dispatch center protected?
  - MDTs & iPads
  - Network & antenna sites

USB PORT AWARENESS

The Deadly USB Stick/Thumb Drive

- It has become an easy route for infection
- Those infections are behind the firewall



Best Practice – Do Not Allow Charging Smartphones via USB

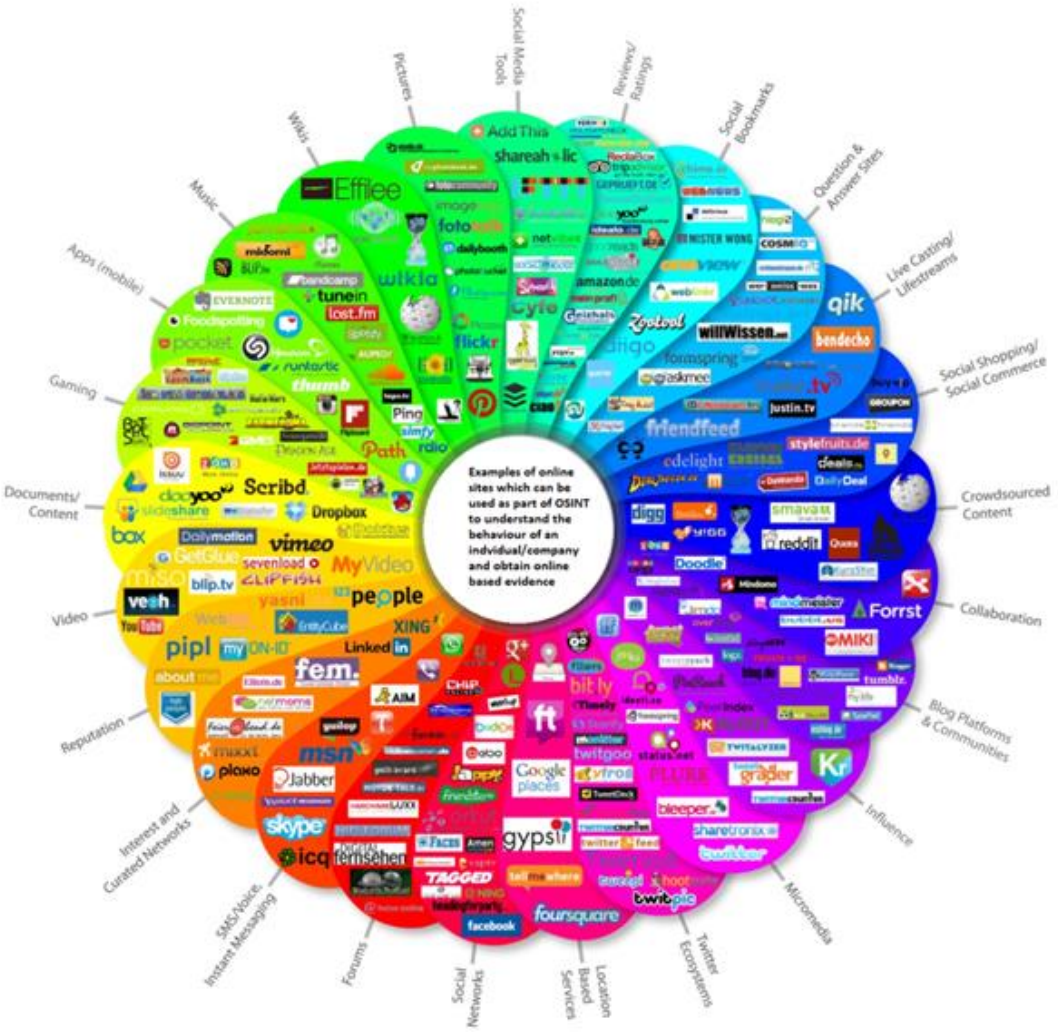
It is recommended that personal smartphones not be allowed to be charged via a USB attached to any computer on the center's network

Recommendation

- Disable USB Ports On PSAP Computers
- Access only possible using an administrative password

SOCIAL MEDIA IN YOUR PSAP/ECC

Social Media = Potential Infection or Attack Vector



Social Media Is Everywhere

- You eliminate the risk of infection through social media only if you completely eliminate employee access to it
- One option, is to set up a separate "public" Wi-Fi that dispatches can also use (vs. Using the agency network for Internet access

Best Practice - Personal Social Media Use on PSAP Workstations

If Allowed:

- Require the use of two factor authentication for login
- Reminders to Staff that Clicking on *Links* May Be Dangerous

Personal Email Use – Same Concerns

Phishing is a major concern

Recommendation

Do Not Allow:

- Social Media
- Personal Web-Based email

on the PSAP Network

CYBER HYGIENE & BEST PRACTICES

What is Cyber Hygiene?

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

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

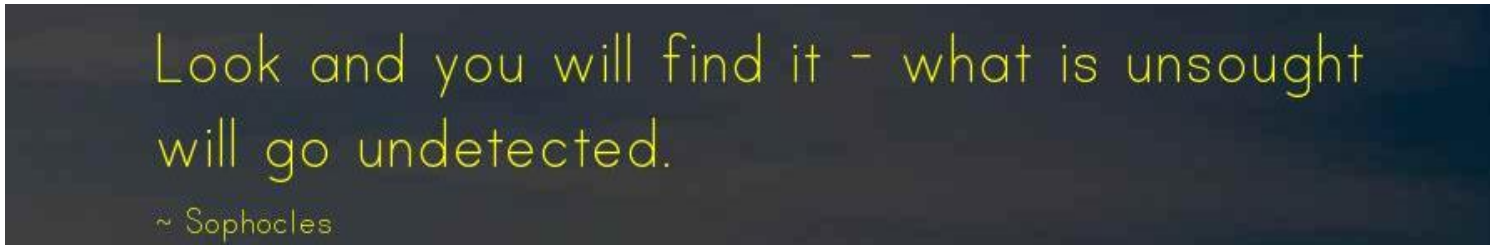
Why This Area Is So Important?

- 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

How Long Does It Take?

A study by the Ponemon Institute revealed the following average days:

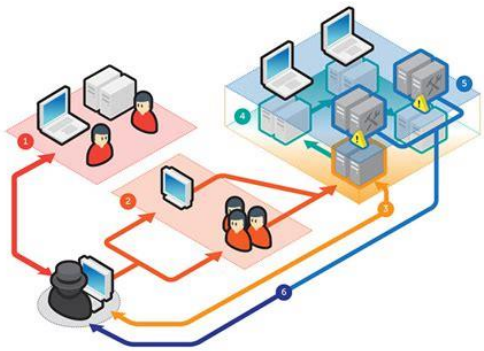
- **Time From Intrusion To Detection**
  206 days
- **Time From Detection To Containment**
  69 days



Why Concern About Personal Computers & Devices?

If I don't use it to access the PSAP/ECC network, why the concern?

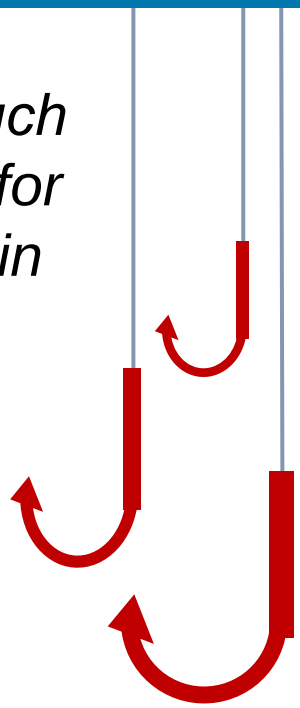
- May not access network, CAD, etc. using your personal computer or device, but probably access the agency network remotely for email or docs/spreadsheets/etc.
- Potential for a Lateral Attack scenario like we discussed earlier



PHISHING

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]"



SPEAR PHISHING

- Phishing messages crafted specifically for an individual target or group

WHALING

- Spear-phishing targeted at high-level, high-value employees

SMISHING

- Phishing attacks conducted over SMS text message on mobile devices rather than e-mail

Cyber Hygiene & Perspectives

- **Cyber hygiene is mostly about changing the habits of users**
- It is okay to say that security is an inconvenience, but we have to learn to work with it efficiently and effectively
- Must understand that we face cyberattacks threats across all communication and collaboration systems
- Balance prevention with detection efforts

It's great to have a car alarm, but you should still lock the doors and take other preventative measures

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

What Is Social Engineering?

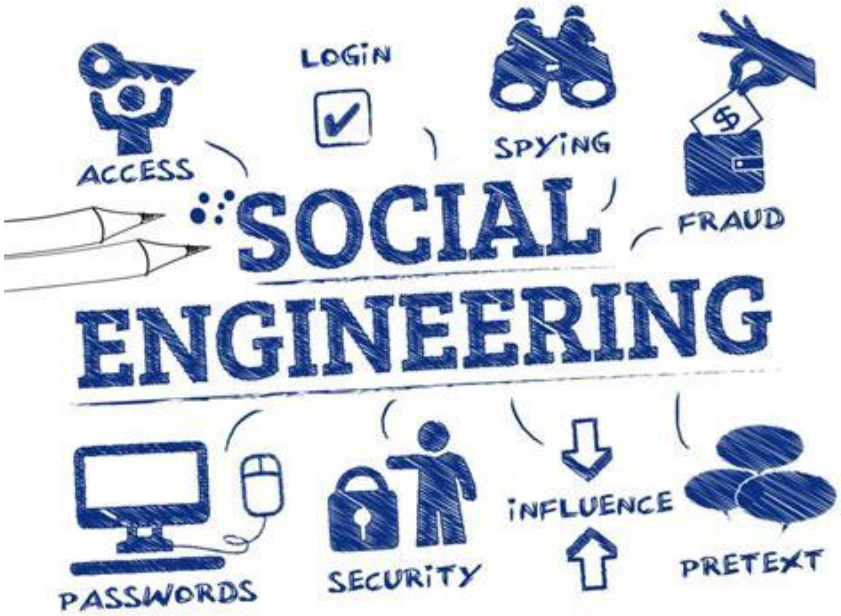
- The term used for a broad range of malicious activities accomplished through human interactions
- It uses psychological manipulation to trick users into making security mistakes that they would not normally do or giving away sensitive information

Social Engineering – How It's Done

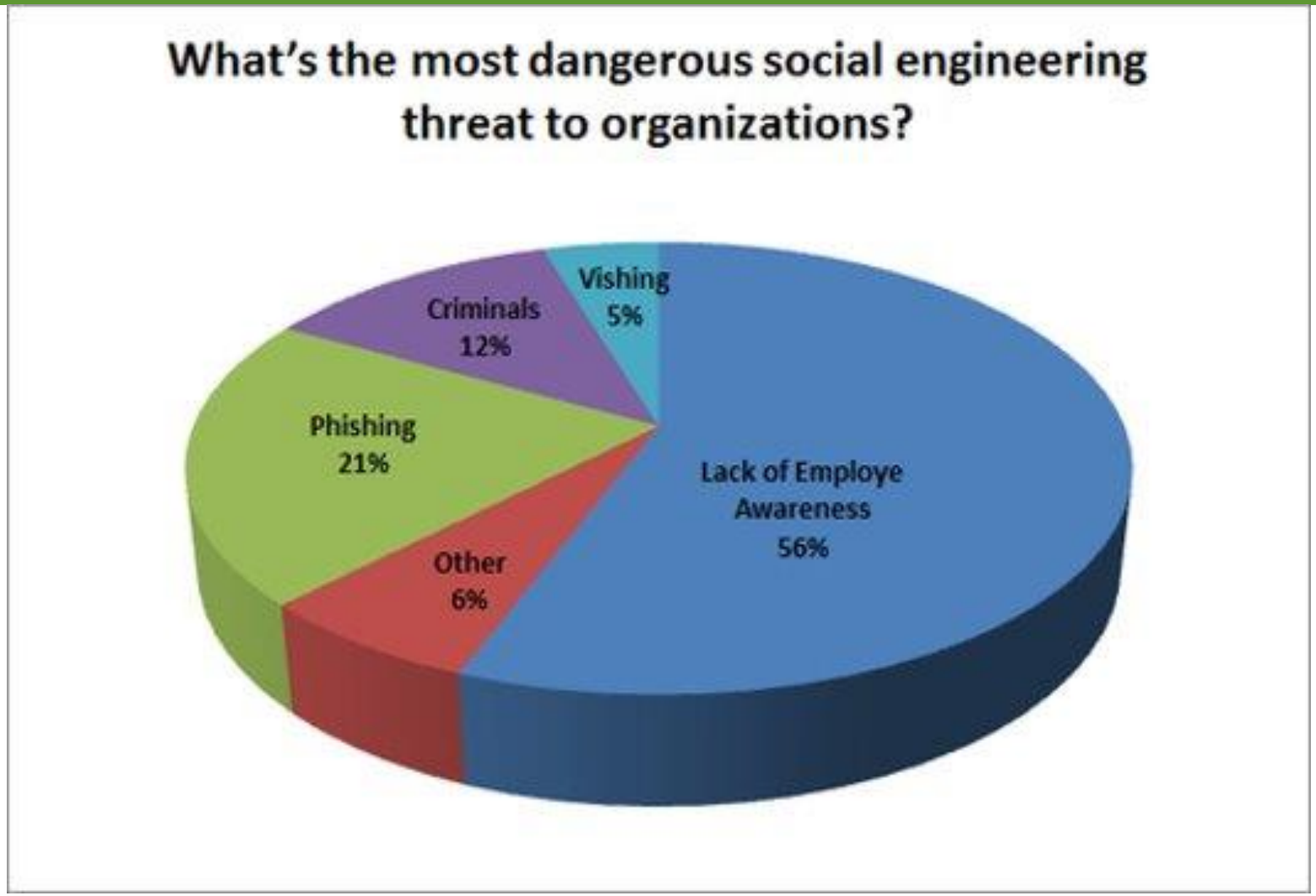
- **Scarcity** – They push people to act/make a decision quickly
- **Dissonance** – People tend to be drawn to and trust people that have similar beliefs, attitudes and values as they do
- **Social Association or Connectedness** – People will do things to belong to or remain a member of a group

Social Engineering – How It's Done

- **Obligation** – When others do something for us, we feel a strong need/obligation to return the favor
- **Self-Esteem** – People generally feel the need to impress and want praise, recognition and/or acceptance



Social Engineering & Training



COVID-19 Phishing – Food For Thought

- Employees working from home don't have the same protections they had while working in their office
- People are very nervous about the virus, are multi-tasking and may have a lot of distractions at home – increases vulnerability
- According to Proofpoint, more than 30% of compromised emails are delivered on Monday as hackers try to capitalize on weekend backlogs

COVID-19 – Cybersecurity/Phishing

- Cyber criminals are using the pandemic to launch cyberattacks
- Not a significant increase in the total volume - They just shifted their focus to Coronavirus theme
- These are not new attack vectors being developed – Just putting on a COVID-19 twist
- Cybercriminals are spoofing organizations that are providing COVID-19 updates to the public
- Ransomware does not seem to be a focus (now)

How Do They Get People To “Bite”?

- **Urgency/Time Sensitive** – Urgent work requirement
- **Scarcity** – You’ll lose your work at home eligibility
- **Personal Health or Importance** – Update on virus in your agency or community

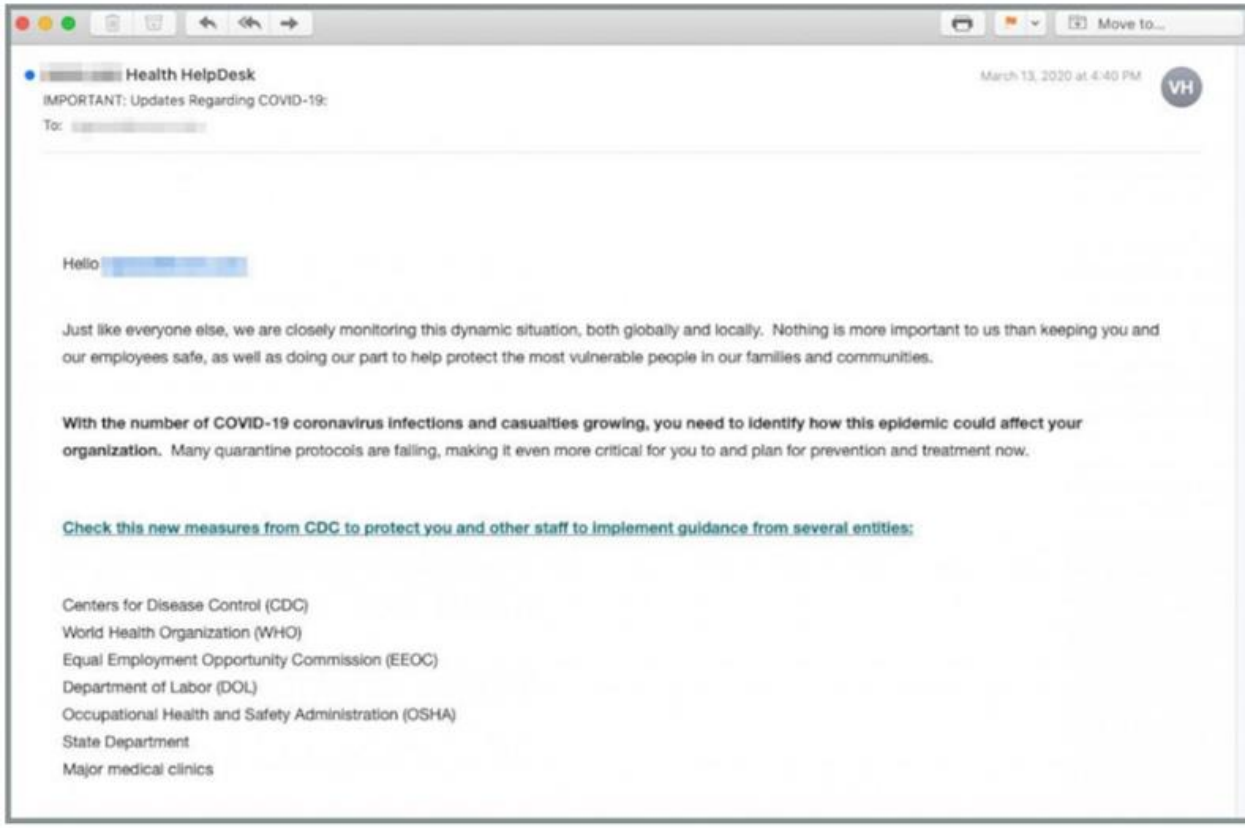
"This is Joe from IT, I'm seeing some issues that could disable your access, let's enter your sign-in info to check it out..."

Examples Of Phishing Attempt Emails

1. **CDC Spoofing**
2. **COVID-19 Update/Cure**
3. **Fake/Infected Attachments**
4. **Credential Theft**

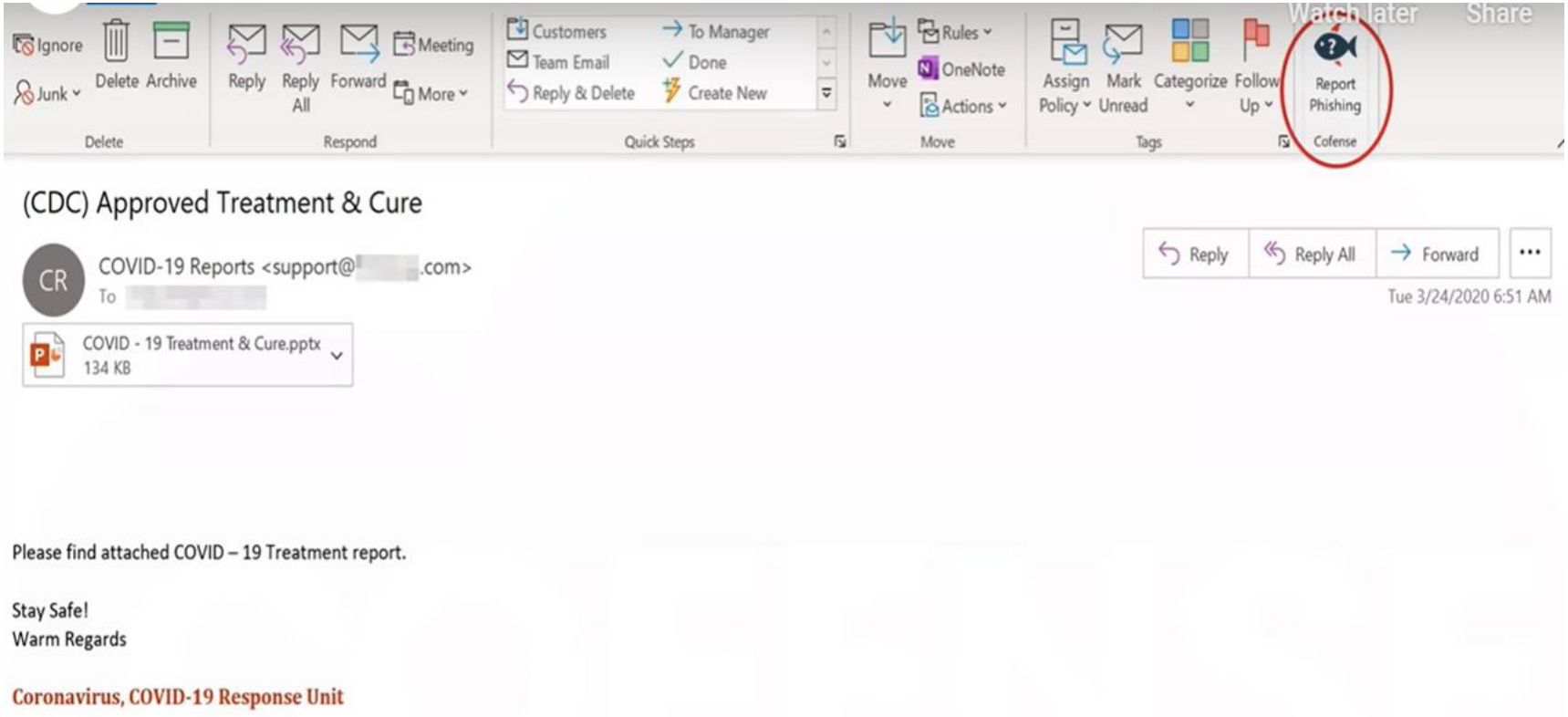
1. CDC Spoofed Email

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



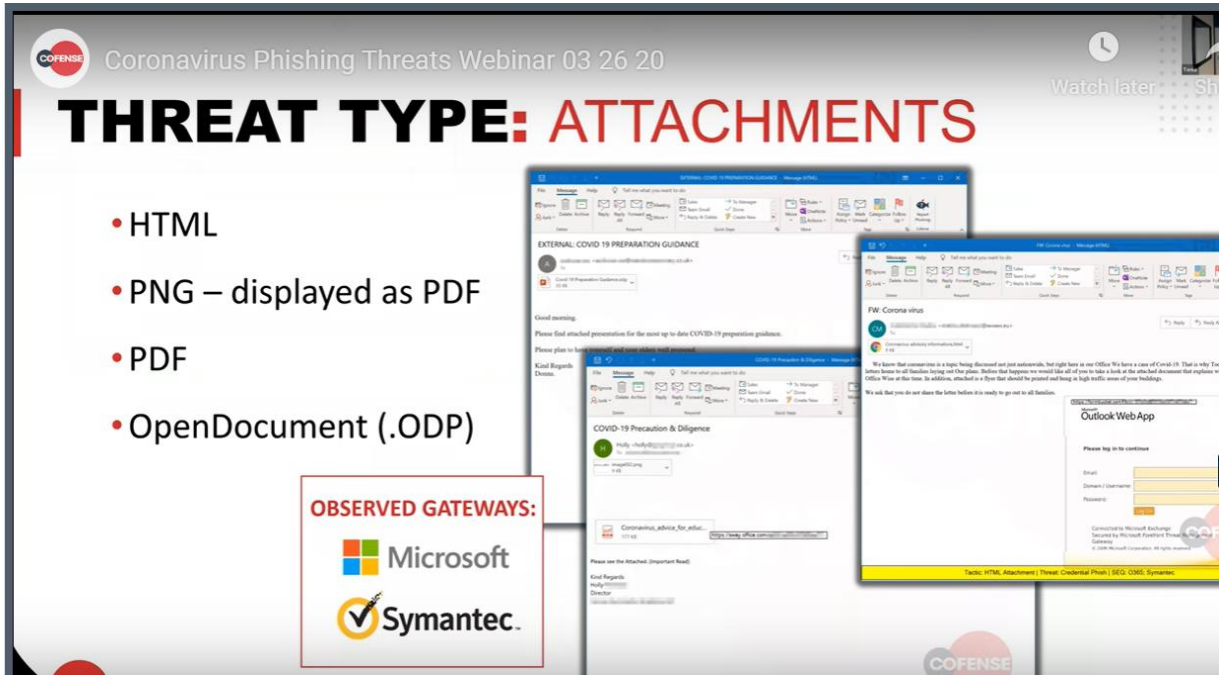
Cybersecurity experts have identified a significant uptick in coronavirus-related phishing scams.
Courtesy of INKY

2. COVID-19 Treatment/Cure Spoofed Email



3. 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



Source: CoFense

4. Credential Theft

- 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

Best Practices – Phishing AND COVID-19 Related

- Remain vigilant and take precautions
- Avoid clicking on links in unsolicited emails and be wary of email attachments – Hover over it so see the source
- Do not respond to email solicitations for personal information
- CISA recommends turning off your email client's option to automatically download attachments

Best Practices – Phishing AND COVID-19 Related

- Use trusted sources—such as legitimate, government websites—for up-to-date, fact-based information about COVID-19
- If a site claims to be an official government publication, check the URL to see if it ends in .gov
- Double-check any links by hovering over them

Best Practices – Phishing AND COVID-19 Related

- Watch out for file extensions in attachments. File.docx.exe or File.pdf.exe are not documents, but executable programs that may harm your computer
- Phishing emails hijacking the user's system through MS-Office 365 have risen dramatically – Includes 3rd Party Outlook Add-Ins
- Be leery when asked for info that you are not used to being asked for

Best Practices – Phishing AND COVID-19 Related

- Review carefully the sender email address – It could it be “spoofed”
- Watch for mistakes in spelling and grammar
- Phishing emails usually use non-personalized greetings

Best Practices – Phishing AND COVID-19 Related

- Do not act if you feel pressured: phishers usually create a sense of urgency
- If in doubt, use out of band verification via phone, SMS or chat
- If you already opened an MS Office that is asking you to “Enable Content”, close and delete that document immediately

Best Practice – Passwords

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

Ag3ofUlTr0n!
1NfiNityW@Rs%tH@N05

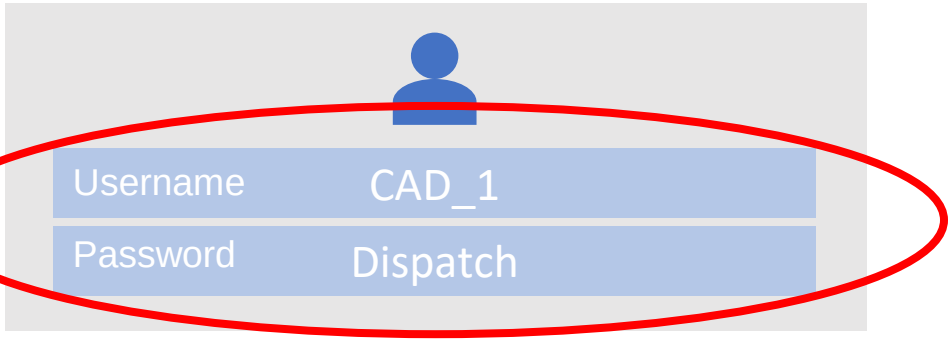
Regularly change passwords & NEVER post passwords where they are visible to other personnel, visitors, or could accidentally be seen in social media posts, etc.

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 – Create 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

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 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!

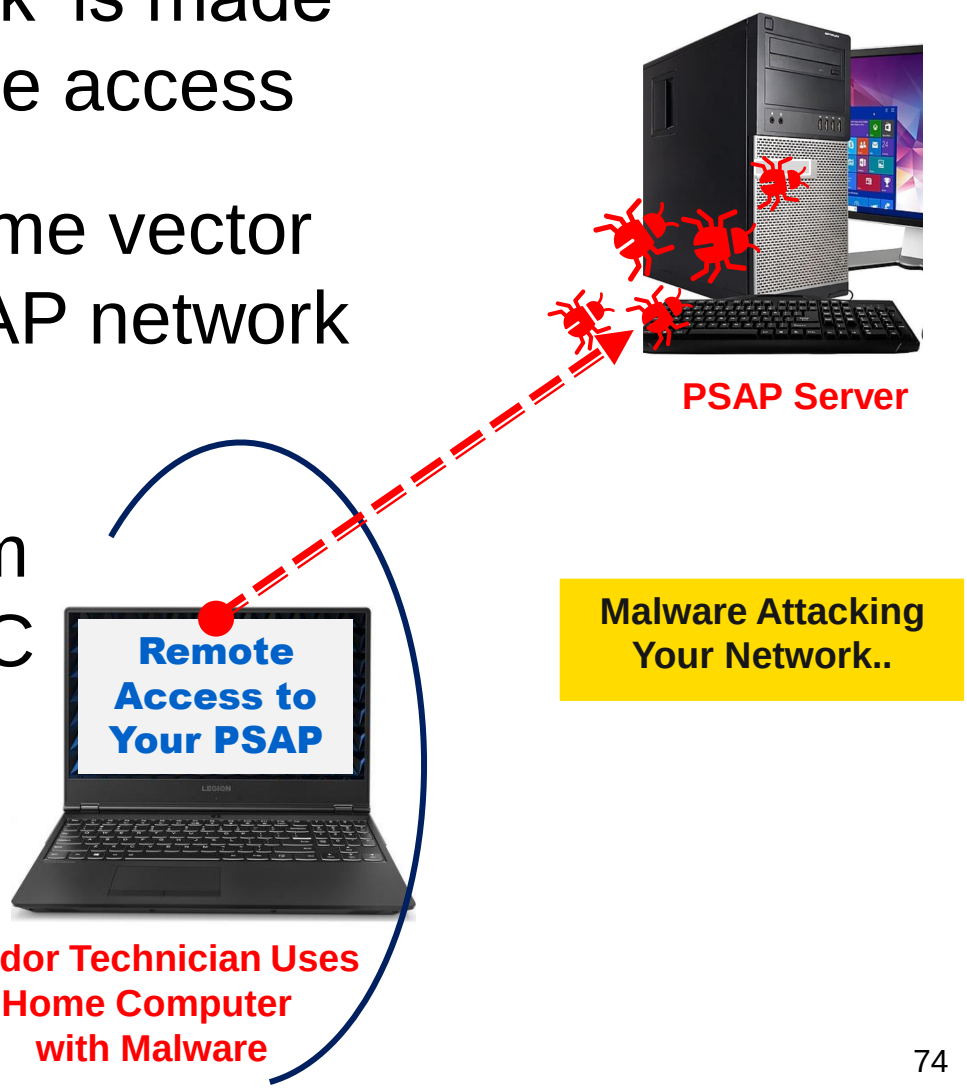
WORKING WITH OUR VENDORS

Vendor Risk

- 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

Dangers of Remote Access

- Any ‘Closed Network’ is made vulnerable by remote access
- Vendors have become vector to attacking the PSAP network
- Target Stores data breach resulted from an attack on a HVAC contractor



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
- How does your vendor handle passwords after an employee event (termination, resignation, promotion, etc.)
- Insist your system have a unique login

RESPONDING TO AND REPORTING CYBER INCIDENTS

Planning For The Inevitable Attack

1. Establish an incident response team
2. Train and exercise the team
3. Create an incident response plan, policy procedures and process
4. Acquire tools and resources

Overall – You Need to Build Incident Response Capabilities

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		

PSAP/ECC Initial Response Actions

1. **Alert** IT and management teams
2. **Disconnect** the infected computer from the network
3. Immediately begin to ensure that **Mission-Critical** systems and information is protected
4. **Backups** (onsite, offsite and in the cloud) should be checked and confirmed to not be affected

PSAP/ECC Initial Response Actions

5. Implement cyber security protocols and convene the Incident Response Team

6. Notify employees of the attack

7. Notify appropriate local, state and federal **law enforcement**

8. Follow any necessary **compliance and/or reporting requirements**

PSAP/ECC Initial Response Actions

9. Notify the public (at the appropriate time) regarding the attack and engage with outside media

10. Utilize non-essential personnel as scribes to document what was done, why it was done, when it was done and who did what

CISA
CYBER+INFRASTRUCTURE

Contact CISA for These No-Cost Resources

- **Information sharing with CISA and MS-ISAC (for SLTT organizations)** includes bi-directional sharing of best practices and network defense information regarding ransomware trends and variants as well as malware that is a precursor to ransomware
- **Policy-oriented or technical assessments** help organizations understand how they can improve their defenses to avoid ransomware infection: https://www.cisa.gov/cyber-resource-hub
  - Assessments include Vulnerability Scanning and Phishing Campaign Assessment
- **Cyber exercises** evaluate or help develop a cyber incident response plan in the context of a ransomware incident scenario
- **CISA Cybersecurity Advisors (CSAs)** advise on best practices and connect you with CISA resources to manage cyber risk
- **Contacts:**
  - **SLTT organizations:** CyberLiaison_SLTT@cisa.dhs.gov
  - **Private sector organizations:** CyberLiaison_Industry@cisa.dhs.gov

CISA Phased Cyber Approach

Use a Cybersecurity Framework

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

	Category
Identify	Asset Management
	Business Environment
	Governance
	Risk Assessment
	Risk Management Strategy
Protect	Access Control
	Awareness and Training
	Data Security
	Information Protection Processes & Procedures
	Maintenance
	Protective Technology
Detect	Anomalies and Events
	Security Continuous Monitoring
	Detection Processes
Respond	Response Planning
	Communications
	Analysis
	Mitigation
	Improvements
Recover	Recovery Planning
	Improvements
	Communications

The Framework – 5 Key Areas

QUESTIONS?

CISA

CYBER+INFRASTRUCTURE