CISA | CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

*IMPLEMENTING THE NECP WEBINARS*

# READY & RESILIENT: CYBER INCIDENT RESPONSE STRATEGIES FOR EMERGENCY COMMUNICATIONS

OCTOBER 25, 2023

**Charlee Hess**
October 25, 2023

# Agenda

- National Emergency Communications Plan (NECP) and SAFECOM Nationwide Survey (SNS): Cyber Posture and Readiness
- Speaker Presentations
- Resources and Actions
- Question and Answer Session

# Speakers

**Charlee Hess**
Planning Branch Chief
Emergency Communications Division
Cybersecurity and Infrastructure Security Agency

**George Perera**
Major, Cyber Crimes Bureau
Miami-Dade Police Department

**Mark Buchholz**

Executive Director
Washington County Consolidated Communications Agency, Oregon

# National Emergency Communications Plan

## NECP Vision

To enable the Nation’s emergency response community to communicate and share information securely across communications technologies in real time, including all levels of government, jurisdictions, disciplines, organizations, and citizens impacted by any threats or hazards event

# National Emergency Communications Plan

**Mandate**
The NECP is mandated by Title XVIII of the Homeland Security Act of 2002 (as amended)

**Guidance**
Provides guidance for those who plan for, coordinate, invest in, and use communications

**Stakeholders**
Helps stakeholders update policies, governance, planning, and protocols

# NECP Goals

Goal 1
**Governance & Leadership**

Goal 2
**Planning & Procedures**

Goal 3
**Training, Exercises, & Evaluation**

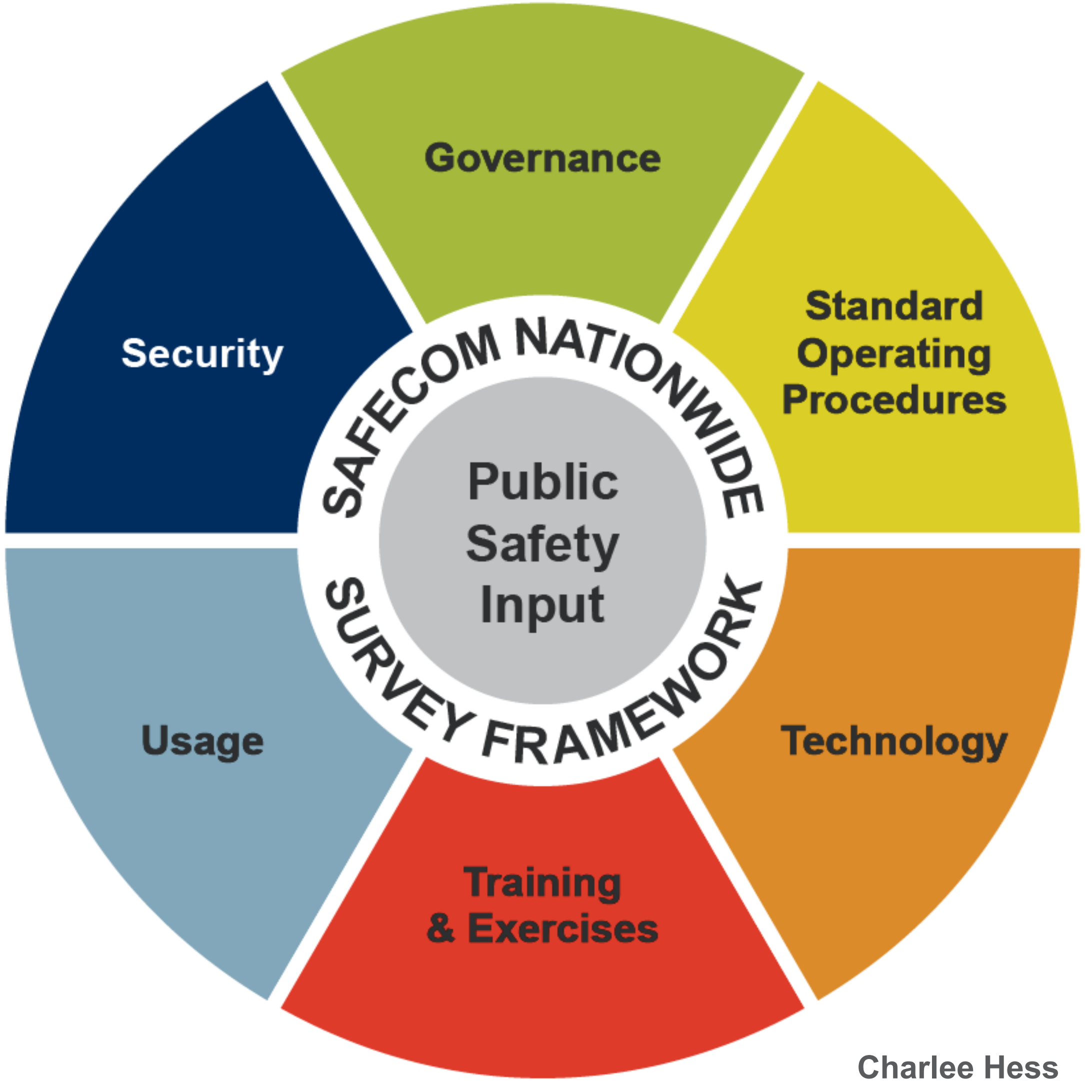
Goal 4
**Communications Coordination**

Goal 5
**Technology & Infrastructure**

Goal 6
**Cybersecurity**

# SAFECOM Nationwide Survey (SNS)

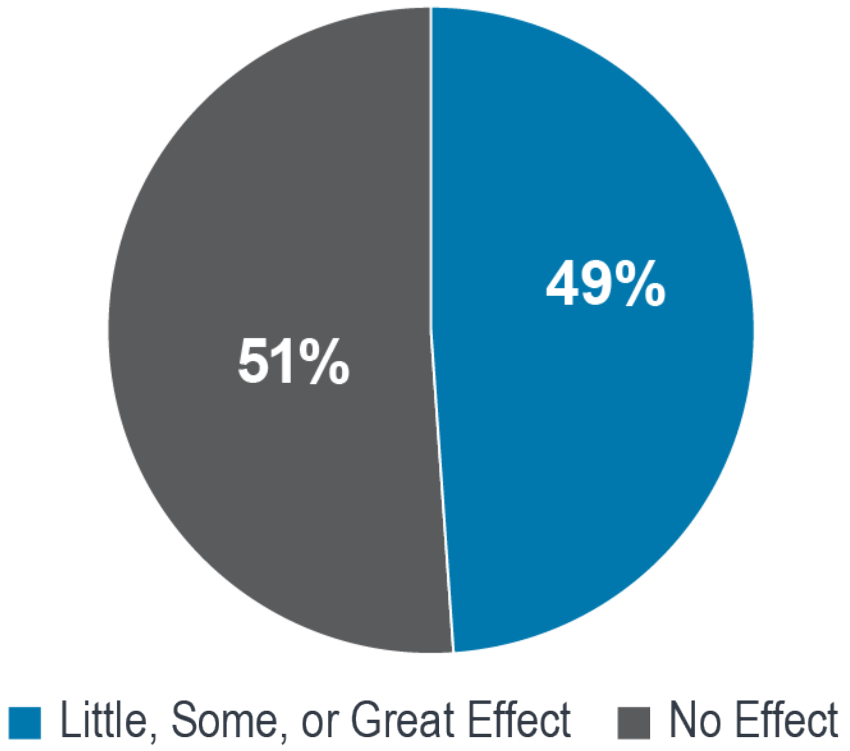
The 2018 SNS consisted of 38 questions that **span the 5 elements of the *SAFECOM Interoperability Continuum***, plus a **security element** that accounted for cybersecurity



# Cybersecurity Overview

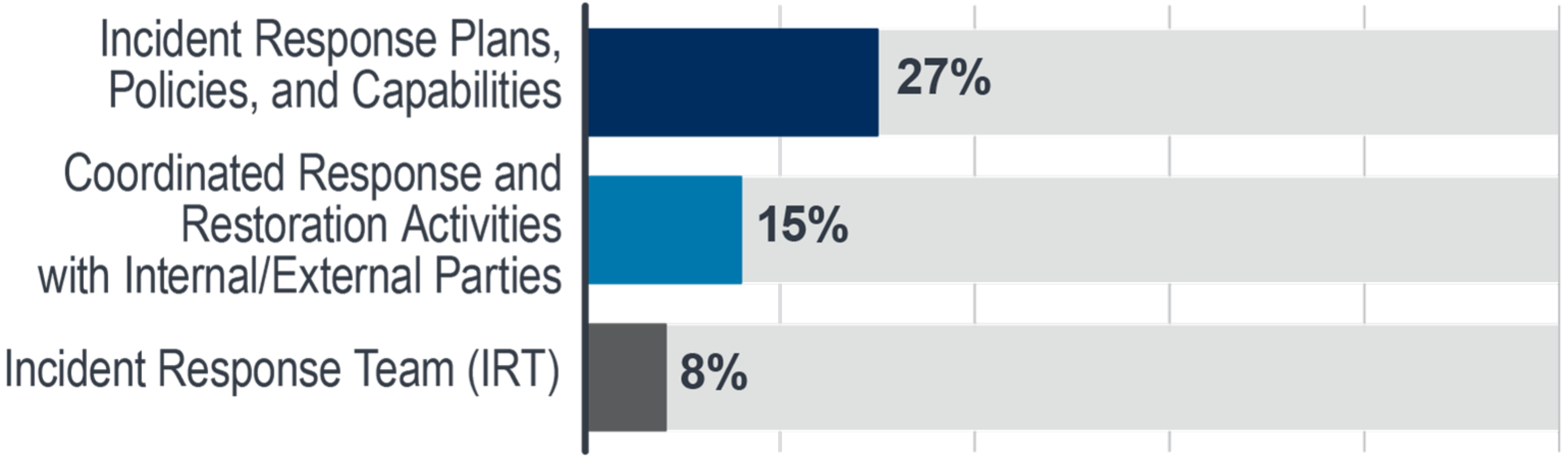
Almost half of SNS respondents reported that a cybersecurity disruption or breach had an effect on their ability to communicate

## Factors that Effect Ability to Communicate: Cybersecurity Disruption or Breach

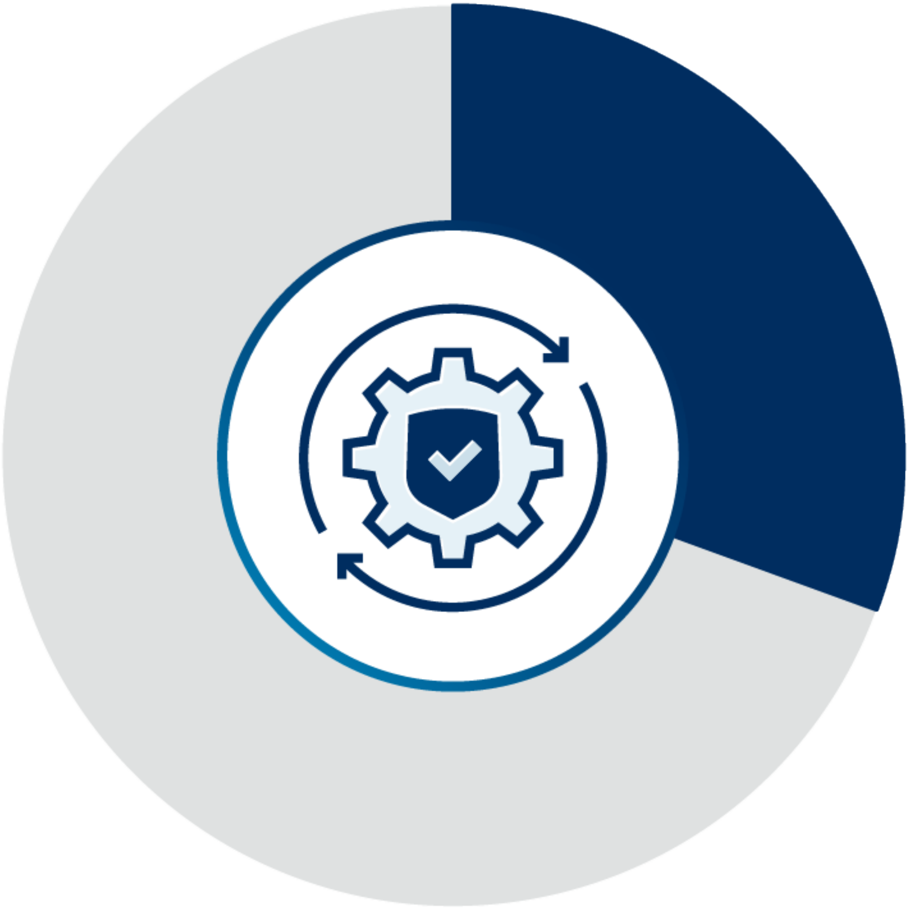


# SNS: Cybersecurity Posture

## Elements Incorporated into Cybersecurity Planning



# SNS: Cybersecurity Posture

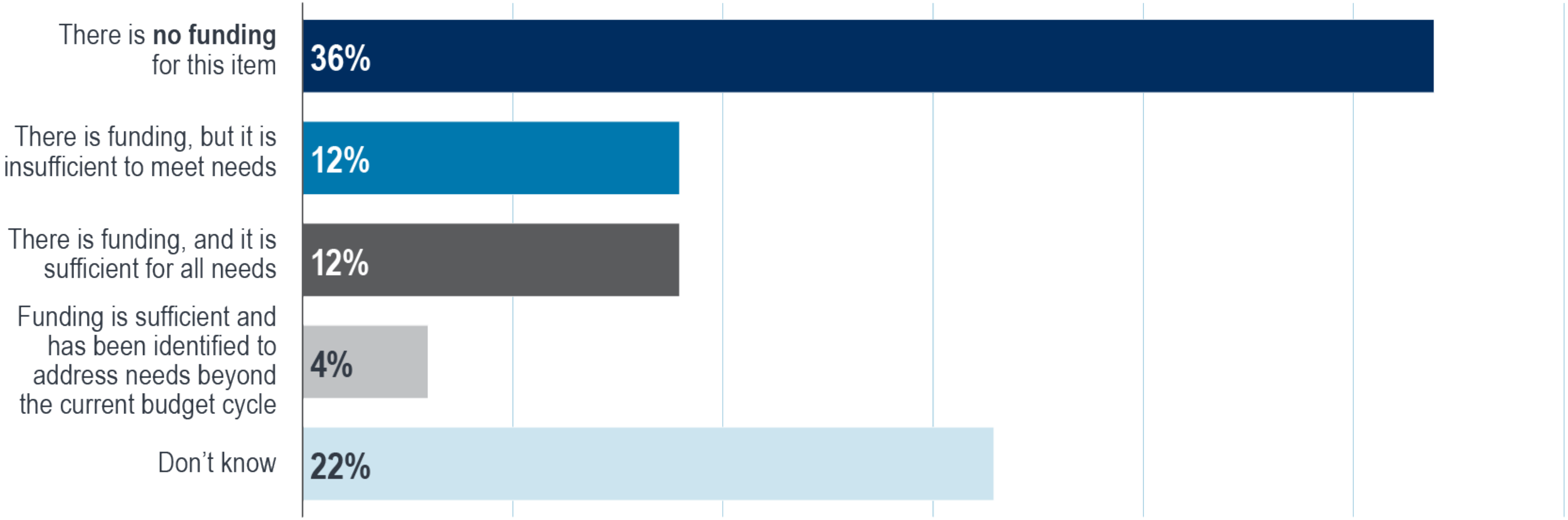


**30.7%**

of SNS respondents conducted no cyber readiness activities

# SNS: Cybersecurity Funding

## Funding for Cybersecurity



# NECP Goal 6: Cybersecurity

**Strengthen the cybersecurity posture of the Emergency Communications Ecosystem**

| | |
|---|---|
| Objective 6.1: | Develop and maintain cybersecurity risk management |
| Objective 6.2: | Mitigate cybersecurity vulnerabilities |
| Objective 6.3: | Determine public safety-specific, standards-based cyber hygiene minimums and fund ongoing risk mitigation |

# Additional Cybersecurity Success Indicators

## Goal 1
**Governance**

- Include network infrastructure and cybersecurity representatives through membership or formalized coordination

## Goal 2
**Planning & Procedures**

- Incorporate risk management strategies into continuity and recovery plans of critical communications

## Goal 3
**Training, Exercises, & Evaluation**

- Update training and exercise programs to address cybersecurity

# Additional Success Indicators

## Goal 4

**Communications Coordination**

- Assess the proficiency of personnel in using communications systems’, features, functions, and capabilities

## Goal 5

**Technology & Infrastructure**

- Support development and implementation of resiliency standards and guidelines

# Speaker Presentations

**George Perera**
Major, Cyber Crimes Bureau
Miami-Dade Police Department

**Mark Buchholz**
Executive Director
Washington County Consolidated Communications Agency, Oregon

# Planning for Continuity in the Face of a Cyber-Attack: Challenges and Best Practices

spam
spoofing
cybersecurity
insider
social
anti-virus
patch
2fa
rootkit
zero-day
vpn
firewall
forensics
response
endpoint
engineering
clickjacking
force
dark
cryptojacking
adware
iam
intrusion
clientless
malware
sandbox
system
identity
advanced
vector
exploit
pii
dpr
persistent
anti-phishing
two-factor
spyware
scareware
infrastructure
ransomware
prevention
detection
authentication
attack
threat
pen
ddos
phishing
anti-malware
vulnerability
backdoor
critical
encryption
assessment
keylogger
virus
anti-botnet
testing
digital
honeypot
spear
protection
iot
web
data
bot
access
botnet
breach
hacker
brute
theft
management

# Three Security Goals

In everything we do

## ✓Confidentiality

Keeping Confidential Data Private

## ✓Integrity

Ensuring Data is Protected From Unauthorized Access or Changes

## ✓Availability

Protect and Ensure System Availability

# Assumptions & Facts

- Everyone is doing what they can to prevent and protect against cyber attacks
    - NIST and CJIS guidelines are your bedtime reading
- There have been a slew of ransom and malware attacks against local governments and school districts in Maryland, Florida, Texas, New York, Atlanta, Dallas…
- Everyone has solid Emergency Operations and Continuity of Operations Plans (COOP), but COOP is not Cyber plan
- Everyone is getting much better at traditional response

### U.S. Marshals Service suffers security breach

The U.S. Marshals Service (USMS) suffered a ransomware security breach this month that compromised sensitive law enforcement information.

### Dangerous China-backed cybercriminals have breached US government in SIX states, experts warn

Experts are warning of a group of cybercriminals that has been targeting state government computer networks in the United States,

### South Florida City Grapples With Ransomware Attack

Pembroke Pines is yet another South Florida city that has fallen victim to a ransomware attack. The attack briefly knocked the city's systems offline, but it remains unknown if any personal data was stolen.

### Florida DEO warns of unemployment data breach

"Malicious actors" may have stolen personal information, such as social security and bank account numbers, in a data breach of Florida's beleaguered unemployment benefits system

### Florida Water Plant Hackers Exploited Old Software And Poor Password Habits

a cyber attacker breached a Florida city’s water treatment plant and tried to poison the water supply. New details about the incident reveal serious cyber security shortcomings at the plant.

# General Cyber attack Types

- Steal info from you or your systems
- Prevent you (or others) from getting info from or using your systems
- Disrupting day-to-day operations

# Cyber Plan

73% of local government organizations have a malware incident recovery plan – the lowest of all sectors surveyed (StateTechMagazine: March 2022)

81% of central government organizations have a malware incident recovery plan – the second lowest of all sectors surveyed (ibid)

Cybercrime cost U.S. businesses more than $6.9 billion in 2021, and only 43% of businesses feel financially prepared to face a cyber-attack in 2022" (Forbes; Alarming Cyber Statistics For Mid-Year 2022 That You Need To Know)

# Complete Plan Contains

## 3 Functional areas

### Policy, Compliance, Architecture, Incident Response

- Develop & Maintain Security Policy
- Vulnerability Management Program
  - System Vulnerability Scanning
  - Application Vulnerability Scanning
- Security Architecture Plan
- Conduct Security Reviews
  - New In-house developed systems
  - Security compliance reviews for procurements
- Conduct internal misuse investigations
- Analyze threat intelligence and alerts received from managed security services provider (MSSP), or other provider ie. Mandiant/FireEye

### Operational Security

- maintain and enhance perimeter security
  - Firewalls (External / Internal / departmental)
  - Load Balancers
- Endpoint Security
- Manage Proxy Infrastructure if used
  - Default blocked websites/categories
  - Implement Blocks as new threats identified
- Secure VPN remote access (encrypted)
- Manage Direct Connect to Cloud Providers and internet connectivity
- Security Event & Information Management
  - Review and respond to alerts
  - Investigate high priority incidents
  - Coordinate response to, contain and remediate incidents

### Identity & Access Management

- Manage identities and access control
  - Office365 and Microsoft Products
  - Keep AD environment patched
  - Manage Enterprise Microsoft OS vulnerability Patching
- Manages email protections
  - spam / av / phishing
  - dmarc / dkim (anti-spoofing)
- Manage Cloud Environment
- Manage Multifactor Authentication for remote access (ie. O365, vpn)
- Information Security Awareness Training
  - General, Annual refresher

# Stealing info from your systems

- Personal Identifiable Information (PII)
- Financial Information
- Protected Healthcare Information (PHI)
- Intellectual Property/Trade Secrets
- Operational Data

# Prevent Users (Or Customers) From Accessing Systems

- Encrypt or erase data from systems (Ransomware)
- Lock systems out while harvesting data or establishing control
- Denial of service (DOS) attacks

# Disrupting Day-To-Day Operations

Crashing vital systems

(9-1-1, CAD, LMR, RMS, telephony, etc.)

Taking down essential infrastructure (power, HVAC, network, radio)

Incapacitating surveillance systems

# Ransomware

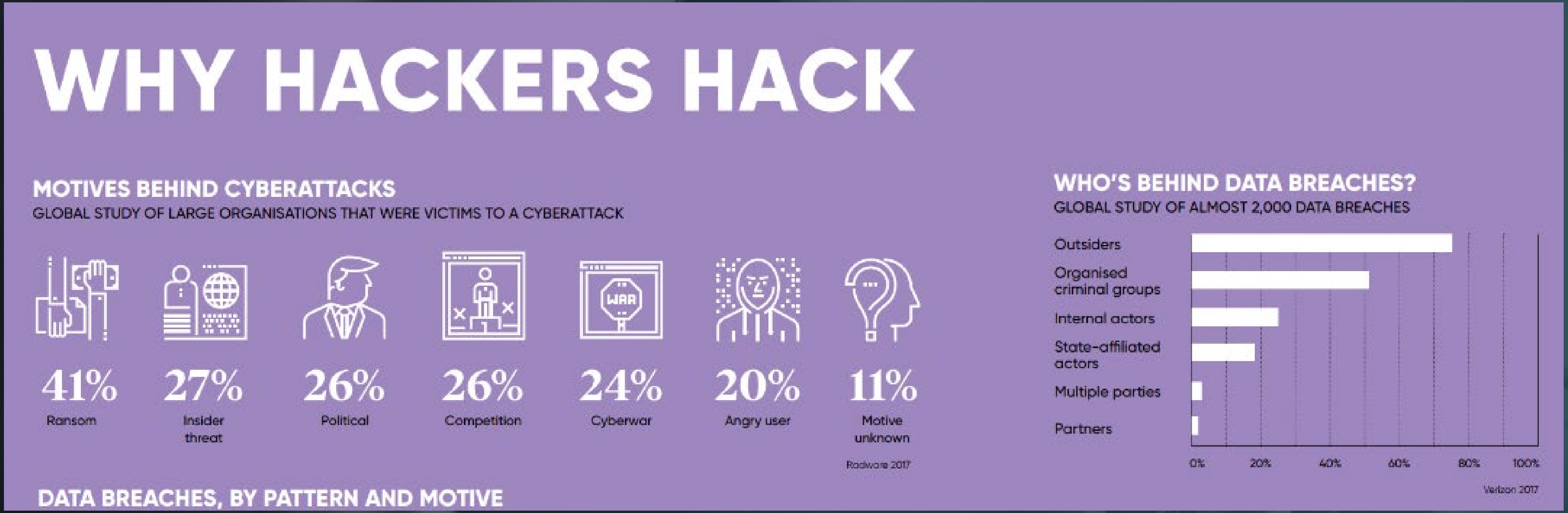
What is ransomware?

It’s a type of malicious software designed to block access to a computer system until a sum of money is paid to the attacker

# Ransomware

- Prevention Strategies
  - Encrypt your data and back it up with an off-line backup
  - Strong passwords for everything (12 or more characters, upper case, lower case, special characters)
  - Don’t reuse passwords – one password per account
  - 2-factor / multi-factor authentication
  - Have a ransomware response plan and practice it!

# Adversary Motivations



## WHY HACKERS HACK

**MOTIVES BEHIND CYBERATTACKS**

GLOBAL STUDY OF LARGE ORGANISATIONS THAT WERE VICTIMS TO A CYBERATTACK

| 41% | 27% | 26% | 26% | 24% | 20% | 11% |
|---|---|---|---|---|---|---|
| Ransom | Insider threat | Political | Competition | Cyberwar | Angry user | Motive unknown |

Radware 2017

**WHO'S BEHIND DATA BREACHES?**

GLOBAL STUDY OF ALMOST 2,000 DATA BREACHES

Verizon 2017

**DATA BREACHES, BY PATTERN AND MOTIVE**

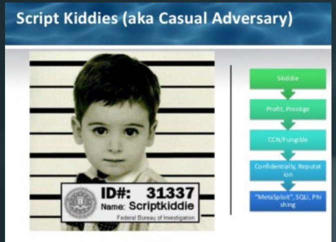
Financial Gain
Fraud

Political Statement

Disrupt and
Destabilize
(Nation State Actors)

Disgruntled Employee
Insider Theft

Thrill and
Notoriety



Script Kiddies (aka Casual Adversary)

ID#: 31337
Name: Scriptkiddie
Federal Bureau of Investigation

Skiddie → Profit, Prestige → CCN/Fungible → Confidentially, Reputation → "MetaSploit", SQLi, Phishing

Damage Critical
Infrastructure
(Nation State Actors)

Cybercrime groups are increasingly running their operations as a business, promoting jobs on the dark web that offer developers and hackers competitive monthly salaries, paid time off, and paid sick leaves. More than 200,000 job ads posted.

# Multi-Layer Defense Security Program

Firewalls (Internal & External)

Anti-Virus
Endpoint Detection and Remediation)

Security Vulnerability and Application Scanning

Security Vulnerability Patching

Email and Content Filtering

Security Event & Information Monitoring

Security Architecture Reviews

Security Policy & Compliance

# Risk Reduction Considerations:

- Assume you will be hit. Ransomware remains highly prevalent. No sector, country, or organization size is immune from the risk. It’s better to be prepared but not hit than the other way round.
- Make backups. Backups are the number one method organizations used to get their data back after an attack. And as we’ve seen, even if you pay the ransom, you rarely get all your data back, so you’ll need to rely on backups either way.
- A simple memory aid for backups is “3-2-1.” You should have at least three different copies (the one you are using now plus two or more spares), using at least two different backup systems (in case one should let you down), and with at least one copy stored offline and preferably offsite (where the crooks can’t tamper with it during an attack).

# Risk Reduction Considerations(cont’d):

- Deploy layered protection. In the face of the considerable increase in extortion-based attacks, it is more important than ever to keep the adversaries out of your environment in the first place. Use layered protection to block attackers at as many points as possible across your environment.
- As much as you can combine human experts and anti-ransomware technology. Key to stopping ransomware is defense in depth that combines dedicated anti-ransomware technology and human-led threat hunting.
- Don’t pay the ransom. We know this is easy to say, but far more difficult to do when your organization has ground to a halt due to a ransomware attack. Independent of any ethical considerations, paying the ransom is an ineffective way to get your data back. If you do decide to pay, be sure to include in your cost/ benefit analysis the expectation that the adversaries will restore, on average, only two-thirds of your files.

# Risk Reduction Considerations(cont’d):

- **Password Manager/Multifactor Identification**
  - Majority of cyber-security specialists agree that password managers are indeed the most secure way to protect your passwords.
  - The only password you’ll need to remember on your password manager is the master password
  - Top password managers encrypts passwords before they leave your device. When they’re on a server, even the provider has no way to decipher them.
  - Automatically creates different password for every need
  - When you sign into your online accounts - a process we call "authentication“
  - When you sign into the account for the first time on a new device or app (like a web browser) you need more than just the username and password. You need a second thing - what we call a second "factor" - to prove who you are.
  - Compromised passwords are one of the most common ways that bad guys can get at your data, your identity, or your money. Using multifactor authentication is one of the easiest ways to make it a lot harder for them.

## Risk Reduction Considerations(cont'd):

- Have a malware recovery plan. The best way to stop a cyberattack from turning into a full breach is to prepare in advance. Organizations that fall victim to an attack often realize they could have avoided a lot of cost, pain, and disruption if they had an incident response plan in place.
- Cyber Insurance
  - Many companies looking to deny coverage
  - Could be issue with MSPs
  - Look to NIST standards
  - Non-Compliance and Unverified Security Standards

# Cyber Incident Response Planning

Cyber incidents will happen!
How we respond is equally as important as preventive measures

- Executive Support
- Role and accountability
- Staffing
- Regular Table-top exercises

- Technology/IR Retainers
- Geo-Political Threats
- Culture - Cybersecurity is a shared responsibility for EVERYONE

# Preparedness is the best defense

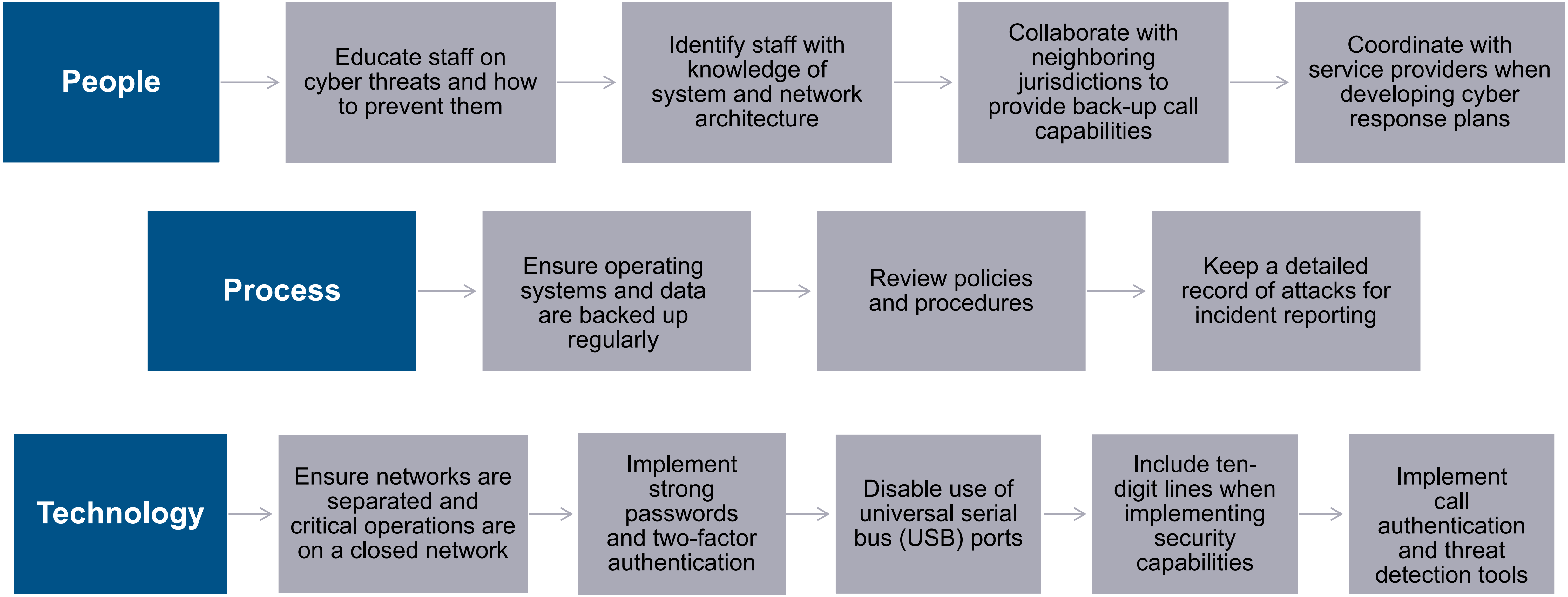
https://www.cisa.gov/cyber-resource-hub
https://www.nist.gov/cybersecurity

## Questions and Answers

Thanks for being here!

George Perera, Major
Miami-Dade Police Department

# Lessons Learned



**People**

- Educate staff on cyber threats and how to prevent them
- Identify staff with knowledge of system and network architecture
- Collaborate with neighboring jurisdictions to provide back-up call capabilities
- Coordinate with service providers when developing cyber response plans

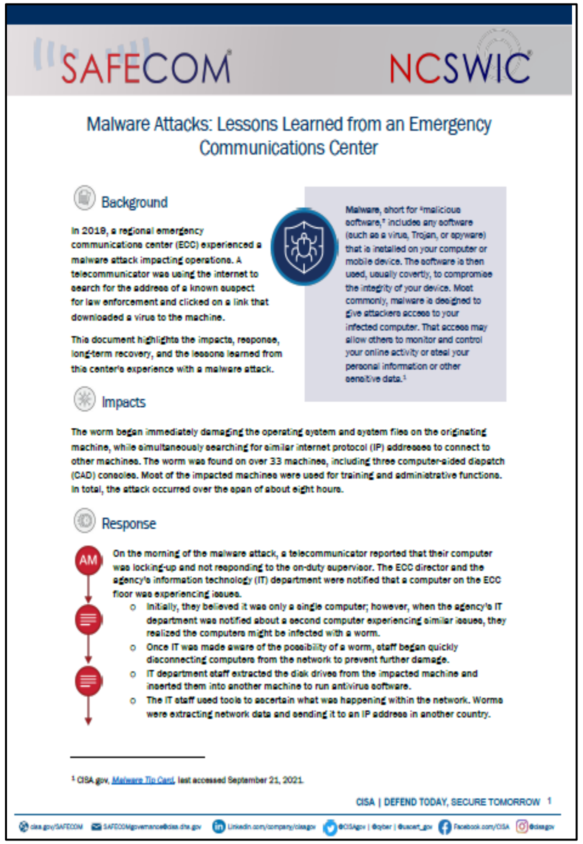
**Process**

- Ensure operating systems and data are backed up regularly
- Review policies and procedures
- Keep a detailed record of attacks for incident reporting

**Technology**

- Ensure networks are separated and critical operations are on a closed network
- Implement strong passwords and two-factor authentication
- Disable use of universal serial bus (USB) ports
- Include ten-digit lines when implementing security capabilities
- Implement call authentication and threat detection tools

# Cyber Incident Response Case Studies



SAFECOM® NCSWIC®

## Malware Attacks: Lessons Learned from an Emergency Communications Center

### Background

In 2019, a regional emergency communications center (ECC) experienced a malware attack impacting operations. A telecommunicator was using the internet to search for the address of a known suspect for law enforcement and clicked on a link that downloaded a virus to the machine.

This document highlights the impacts, response, long-term recovery, and the lessons learned from this center's experience with a malware attack.

Malware, short for "malicious software," includes any software (such as a virus, Trojan, or spyware) that is installed on your computer or mobile device. The software is then used, usually covertly, to compromise the integrity of your device. Most commonly, malware is designed to give attackers access to your infected computer. That access may allow others to monitor and control your online activity or steal your personal information or other sensitive data.[1]

### Impacts

The worm began immediately damaging the operating system and system files on the originating machine, while simultaneously searching for similar internet protocol (IP) addresses to connect to other machines. The worm was found on over 33 machines, including three computer-aided dispatch (CAD) consoles. Most of the impacted machines were used for training and administrative functions. In total, the attack occurred over the span of about eight hours.

### Response

AM

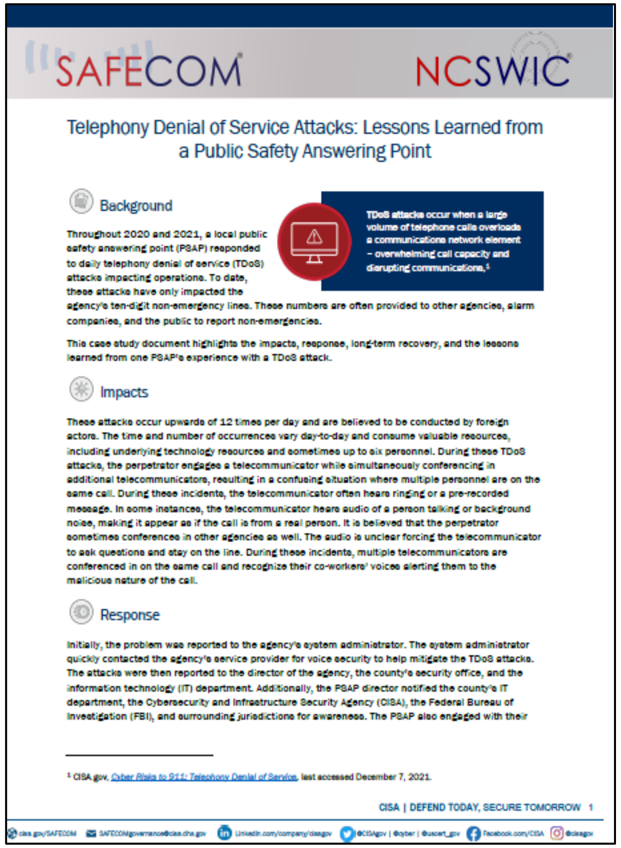
On the morning of the malware attack, a telecommunicator reported that their computer was locking-up and not responding to the on-duty supervisor. The ECC director and the agency's information technology (IT) department were notified that a computer on the ECC floor was experiencing issues.

- Initially, they believed it was only a single computer; however, when the agency's IT department was notified about a second computer experiencing similar issues, they realized the computers might be infected with a worm.
- Once IT was made aware of the possibility of a worm, staff began quickly disconnecting computers from the network to prevent further damage.
- IT department staff extracted the disk drives from the impacted machine and inserted them into another machine to run antivirus software.
- The IT staff used tools to ascertain what was happening within the network. Worms were extracting network data and sending it to an IP address in another country.

[1] CISA.gov, Malware Tip Card, last accessed September 21, 2021.

CISA | DEFEND TODAY, SECURE TOMORROW 1

cisa.gov/SAFECOM SAFECOMgovernance@cisa.dhs.gov Linkedin.com/company/cisagov @CISAgov | @cyber | @uscert_gov Facebook.com/CISA @cisagov



SAFECOM® NCSWIC®

## Telephony Denial of Service Attacks: Lessons Learned from a Public Safety Answering Point

### Background

TDoS attacks occur when a large volume of telephone calls overloads a communications network element – overwhelming call capacity and disrupting communications.[1]

Throughout 2020 and 2021, a local public safety answering point (PSAP) responded to daily telephony denial of service (TDoS) attacks impacting operations. To date, these attacks have only impacted the agency's ten-digit non-emergency lines. These numbers are often provided to other agencies, alarm companies, and the public to report non-emergencies.

This case study document highlights the impacts, response, long-term recovery, and the lessons learned from one PSAP's experience with a TDoS attack.

### Impacts

These attacks occur upwards of 12 times per day and are believed to be conducted by foreign actors. The time and number of occurrences vary day-to-day and consume valuable resources, including underlying technology resources and sometimes up to six personnel. During these TDoS attacks, the perpetrator engages a telecommunicator while simultaneously conferencing in additional telecommunicators, resulting in a confusing situation where multiple personnel are on the same call. During these incidents, the telecommunicator often hears ringing or a pre-recorded message. In some instances, the telecommunicator hears audio of a person talking or background noise, making it appear as if the call is from a real person. It is believed that the perpetrator sometimes conferences in other agencies as well. The audio is unclear forcing the telecommunicator to ask questions and stay on the line. During these incidents, multiple telecommunicators are conferenced in on the same call and recognize their co-workers' voices alerting them to the malicious nature of the call.

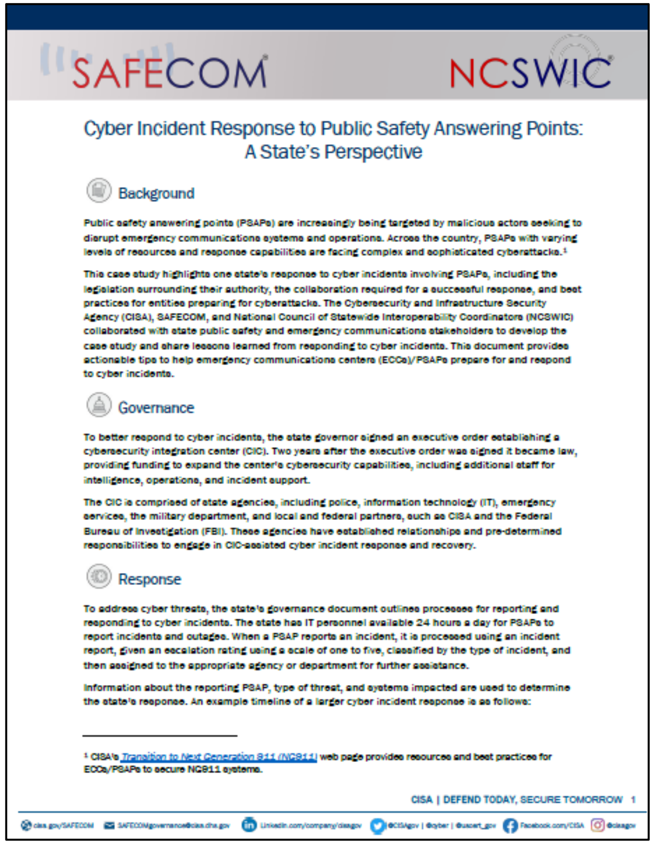
### Response

Initially, the problem was reported to the agency's system administrator. The system administrator quickly contacted the agency's service provider for voice security to help mitigate the TDoS attacks. The attacks were then reported to the director of the agency, the county's security office, and the information technology (IT) department. Additionally, the PSAP director notified the county's IT department, the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and surrounding jurisdictions for awareness. The PSAP also engaged with their

[1] CISA.gov, Cyber Risks to 911: Telephony Denial of Service, last accessed December 7, 2021.

CISA | DEFEND TODAY, SECURE TOMORROW 1

cisa.gov/SAFECOM SAFECOMgovernance@cisa.dhs.gov Linkedin.com/company/cisagov @CISAgov | @cyber | @uscert_gov Facebook.com/CISA @cisagov



SAFECOM® NCSWIC®

## Cyber Incident Response to Public Safety Answering Points: A State's Perspective

### Background

Public safety answering points (PSAPs) are increasingly being targeted by malicious actors seeking to disrupt emergency communications systems and operations. Across the country, PSAPs with varying levels of resources and response capabilities are facing complex and sophisticated cyberattacks.[1]

This case study highlights one state's response to cyber incidents involving PSAPs, including the legislation surrounding their authority, the collaboration required for a successful response, and best practices for entities preparing for cyberattacks. The Cybersecurity and Infrastructure Security Agency (CISA), SAFECOM, and National Council of Statewide Interoperability Coordinators (NCSWIC) collaborated with state public safety and emergency communications stakeholders to develop the case study and share lessons learned from responding to cyber incidents. This document provides actionable tips to help emergency communications centers (ECCs)/PSAPs prepare for and respond to cyber incidents.

### Governance

To better respond to cyber incidents, the state governor signed an executive order establishing a cybersecurity integration center (CIC). Two years after the executive order was signed it became law, providing funding to expand the center's cybersecurity capabilities, including additional staff for intelligence, operations, and incident support.

The CIC is comprised of state agencies, including police, information technology (IT), emergency services, the military department, and local and federal partners, such as CISA and the Federal Bureau of Investigation (FBI). These agencies have established relationships and pre-determined responsibilities to engage in CIC-assisted cyber incident response and recovery.

### Response

To address cyber threats, the state's governance document outlines processes for reporting and responding to cyber incidents. The state has IT personnel available 24 hours a day for PSAPs to report incidents and outages. When a PSAP reports an incident, it is processed using an incident report, given an escalation rating using a scale of one to five, classified by the type of incident, and then assigned to the appropriate agency or department for further assistance.

Information about the reporting PSAP, type of threat, and systems impacted are used to determine the state's response. An example timeline of a larger cyber incident response is as follows:

[1] CISA's Transition to Next Generation 911 (NG911) web page provides resources and best practices for ECCs/PSAPs to secure NG911 systems.

CISA | DEFEND TODAY, SECURE TOMORROW 1

cisa.gov/SAFECOM SAFECOMgovernance@cisa.dhs.gov Linkedin.com/company/cisagov @CISAgov | @cyber | @uscert_gov Facebook.com/CISA @cisagov

Available at: cisa.gov/safecom/next-generation-911

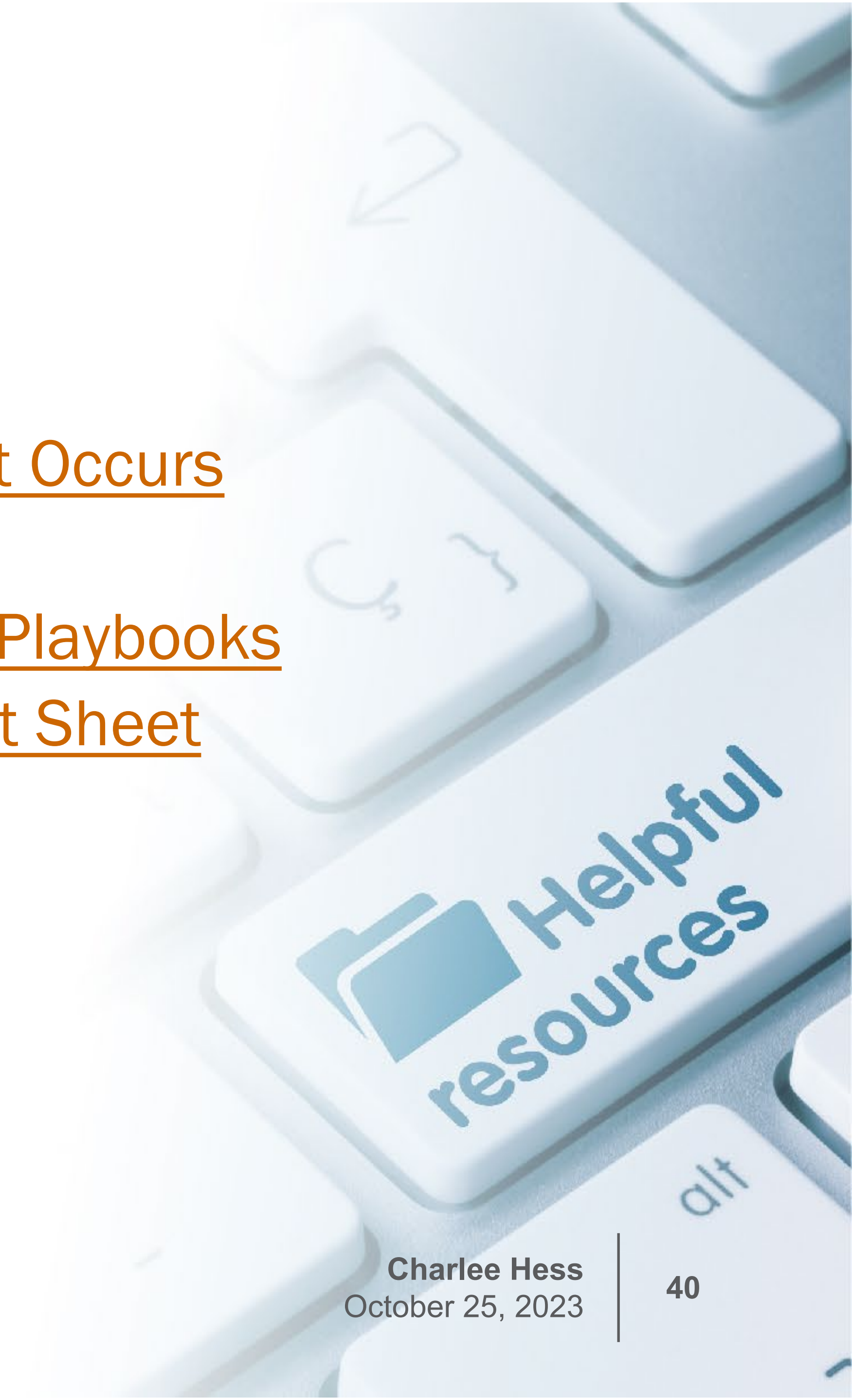
# Cybersecurity Resources for Public Safety

**Find additional cybersecurity resources specifically for public safety at:** cisa.gov/public-safety-cybersecurity

- *Two Things Every 911 Center Should Do to Improve Cybersecurity*
- *Cyber Risks to 911: Telephony Denial of Service*
- *Guide to Getting Started with a Cybersecurity Risk Assessment*
- *“First 48”: What to Expect When a Cyber Incident Occurs*
- *Interoperable Communications Technical Assistance Program Service Offerings Guide*

# Resources

- National Emergency Communications Plan
- SAFECOM Nationwide Survey
- “First 48”: What to Expect When a Cyber Incident Occurs
- Communications and Cyber Resiliency Toolkit
- Cybersecurity Incident & Vulnerability Response Playbooks
- Cyber Resiliency Resources for Public Safety Fact Sheet
- Incident Response Training
- Cyber Essentials Toolkit
- Transition to Next Generation 911 (NG911)
- Public Safety Cybersecurity



# How You Can Take Action

- **Take steps** for your organization or jurisdiction to implement the NECP and achieve its cyber-related success indicators
- **Leverage** available resources to help develop and maintain cyber incident response plans
- **Collaborate** with subject matter experts to assist with cyber incident response activities

# Questions?

# Upcoming Webinars

Join the Cybersecurity and Infrastructure Security Agency for webinars focused on:

## Implementing the National Emergency Communications Plan

Bookmark our webpage to check back for future webinars: **https://www.cisa.gov/necp-webinars**

For more information on the NECP:

www.cisa.gov/necp

NECP@cisa.dhs.gov

CYBERSECURITY & INFRASTRUCTURE

CISA

SECURITY AGENCY