IMPLEMENTING THE NECP WEBINARS

ADDRESSING THE RANSOMWARE THREAT TO EMERGENCY COMMUNICATIONS

OCTOBER 26, 2021

Agenda

- National Emergency Communications Plan (NECP) and SAFECOM Nationwide Survey (SNS): Cybersecurity
- Ransomware
- Resources and Actions
- Question and Answer Session

Presenters

Charlee Hess
Cybersecurity and Infrastructure Security Agency

Amy Nicewick
Cybersecurity and Infrastructure Security Agency

Mark Hogan
City of Tulsa

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 events

National Emergency Communications Plan

Mandate
The NECP is mandated by Title XVIII of the Homeland Security Act of 2002

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

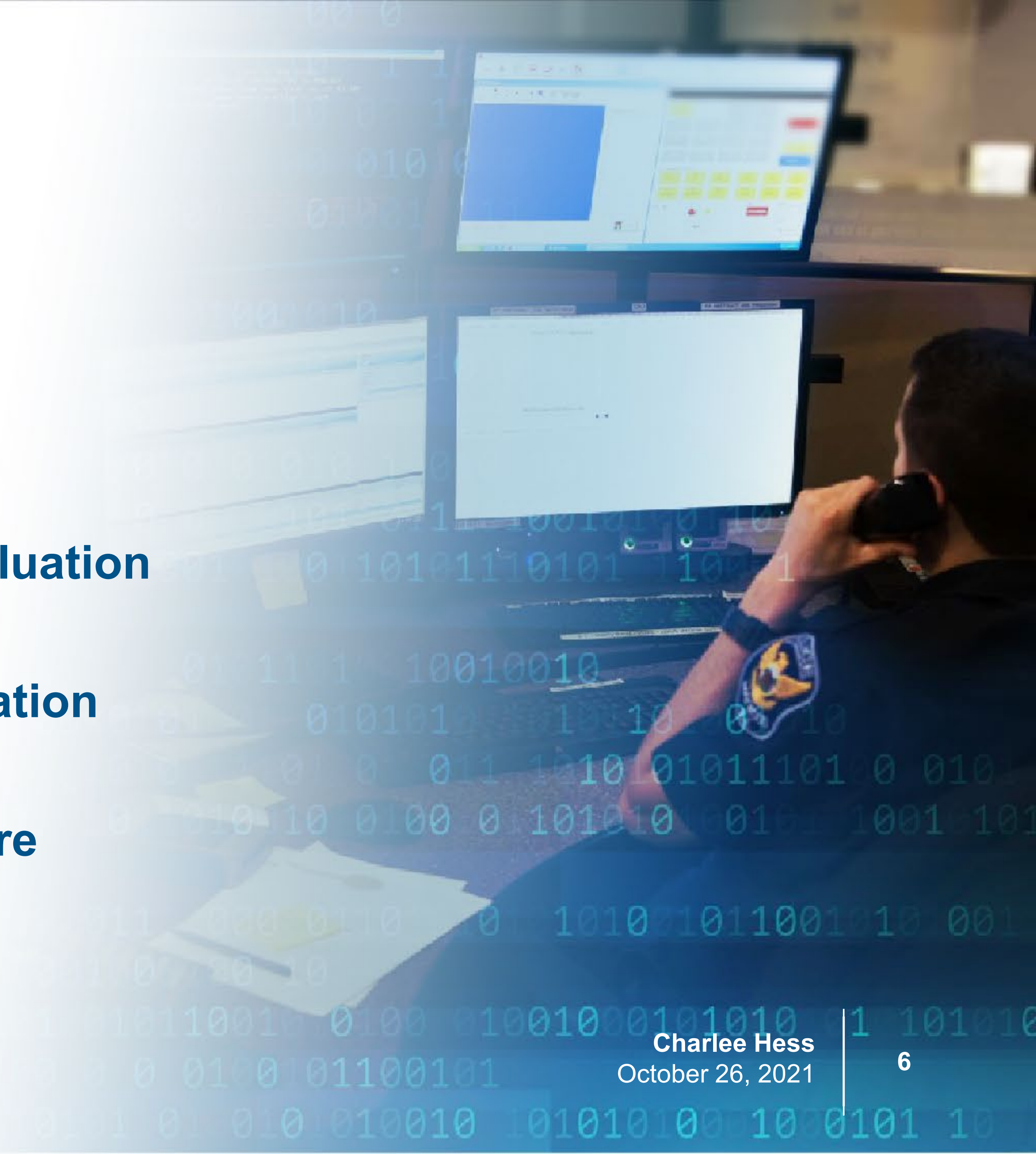
Goal 2
Planning & Procedures

Goal 3
Training, Exercises, & Evaluation

Goal 4
Communications Coordination

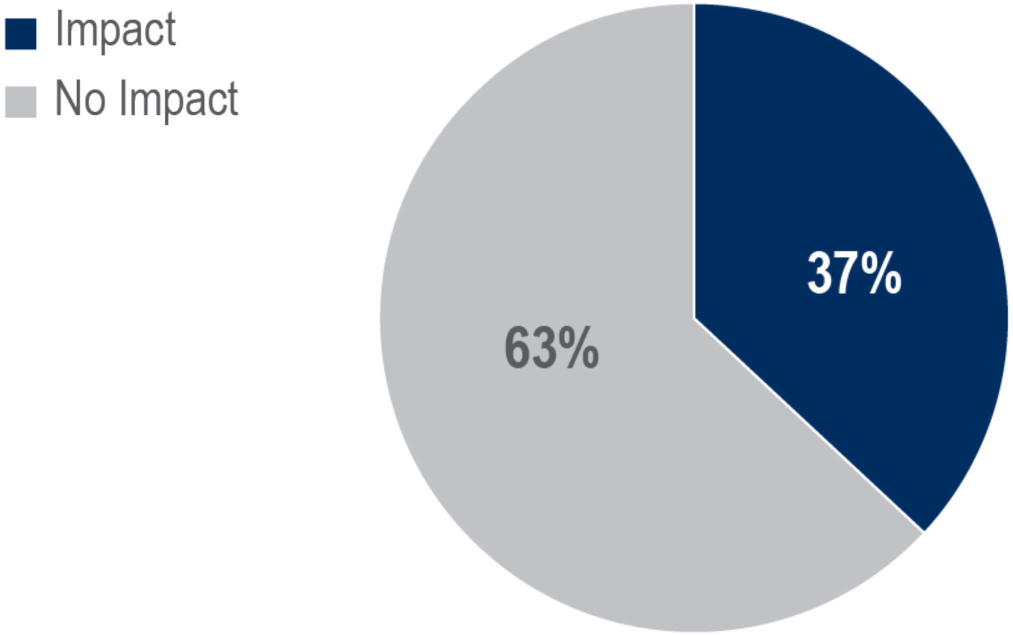
Goal 5
Technology & Infrastructure

Goal 6
Cybersecurity

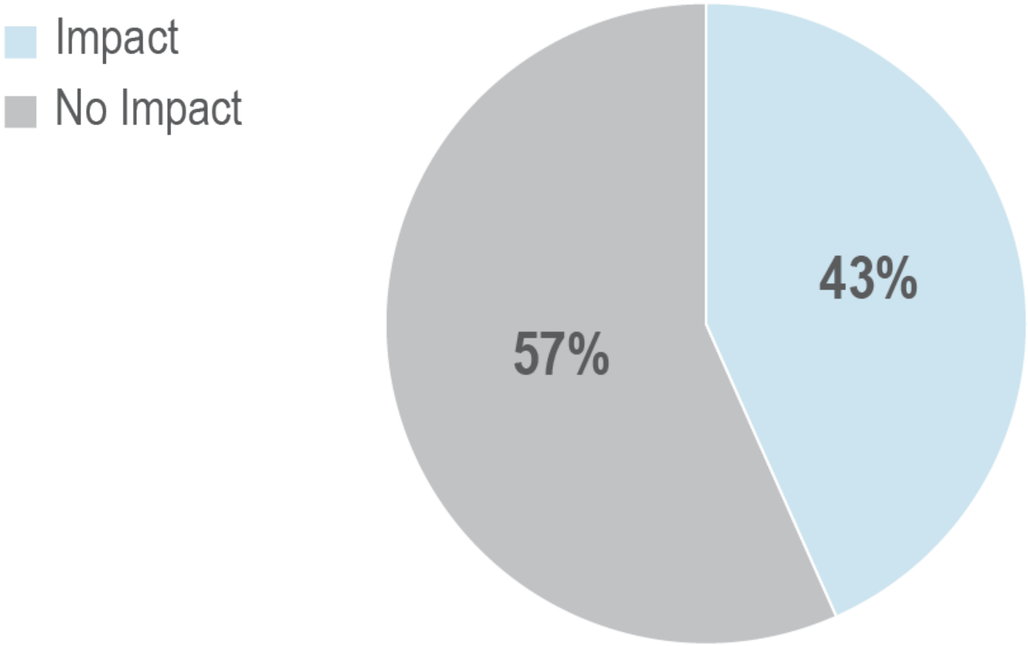


Cybersecurity Overview

Organizations that have Experienced a Cyber Impact

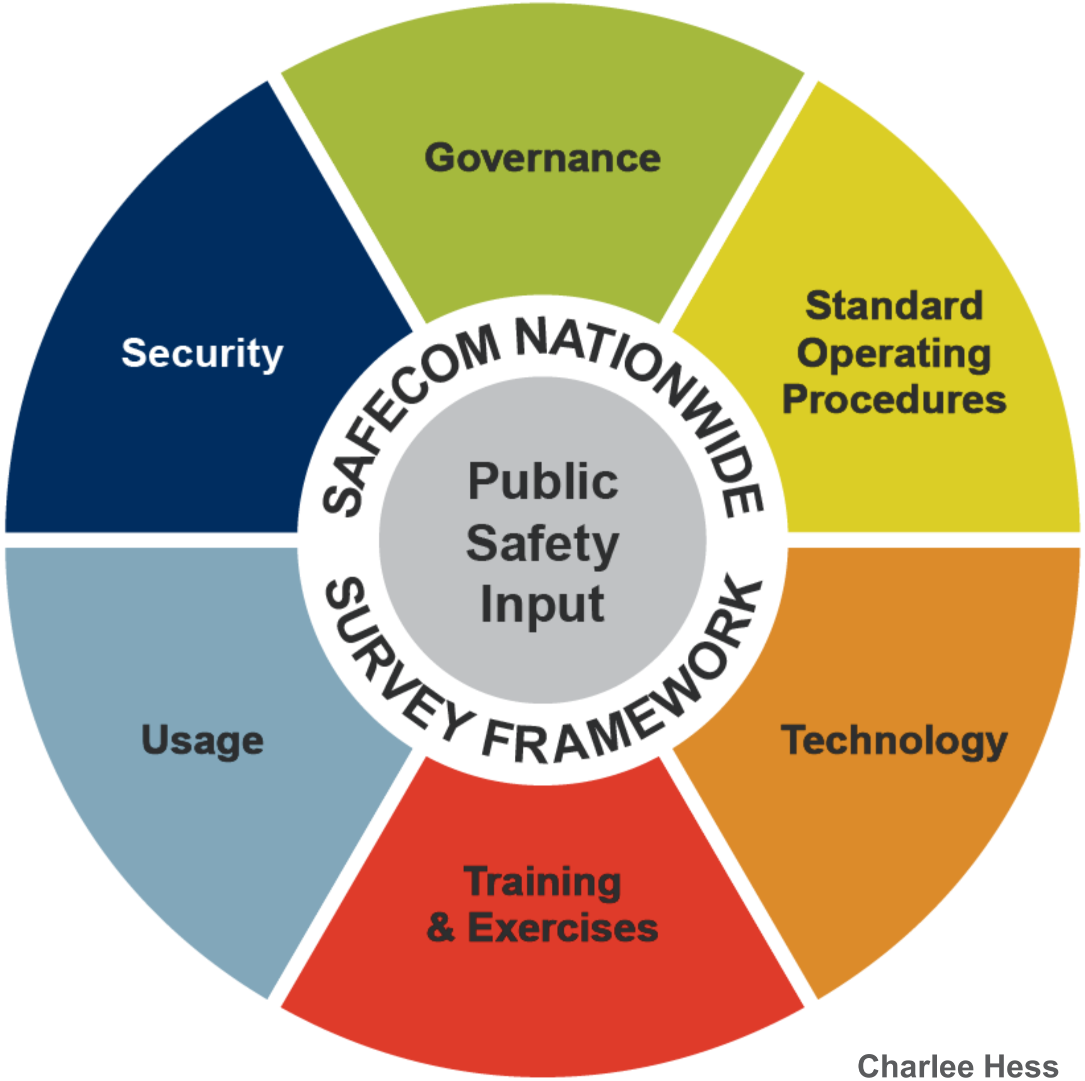


Factors that Affect Ability to Communicate: Cybersecurity Disruption or Breach



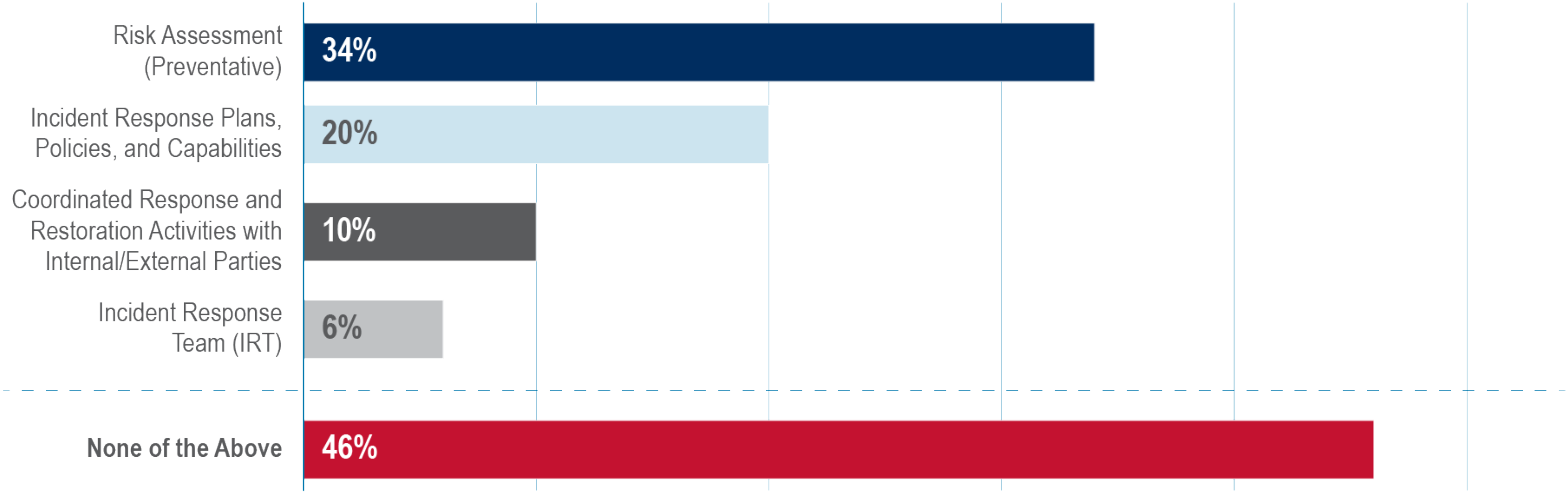
SAFECOM Nationwide Survey (SNS)

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



SNS: Cybersecurity Planning

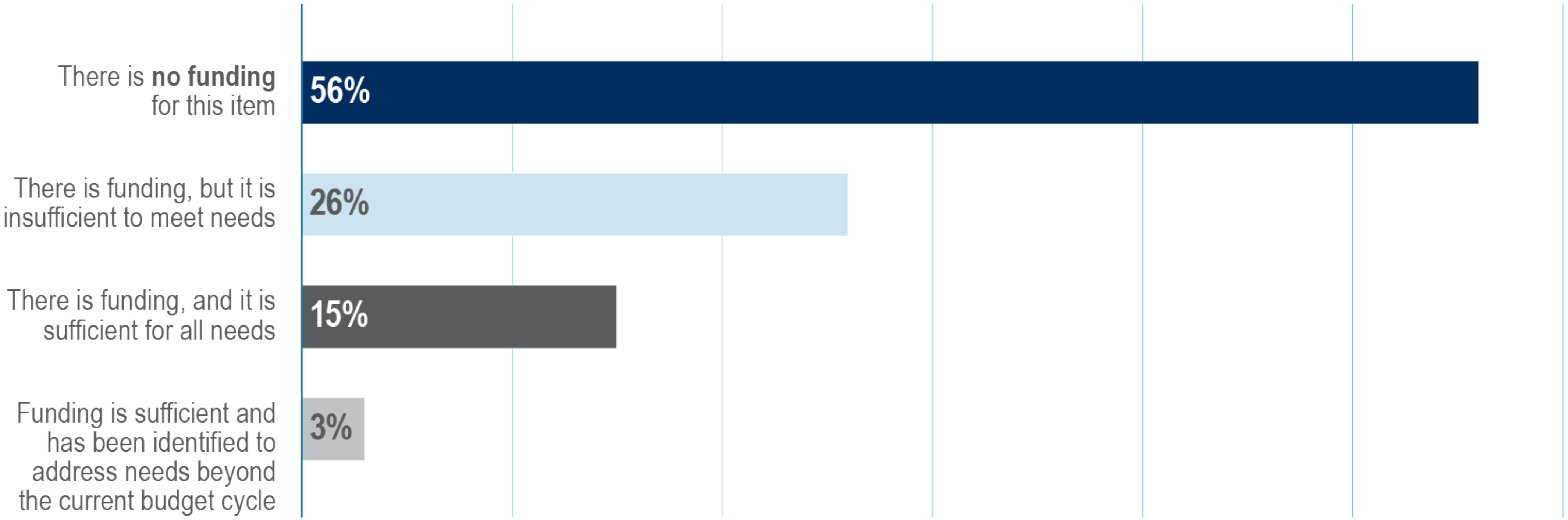
Elements that Organizations Incorporate into Cybersecurity Planning



Charlee Hess
October 26, 2021

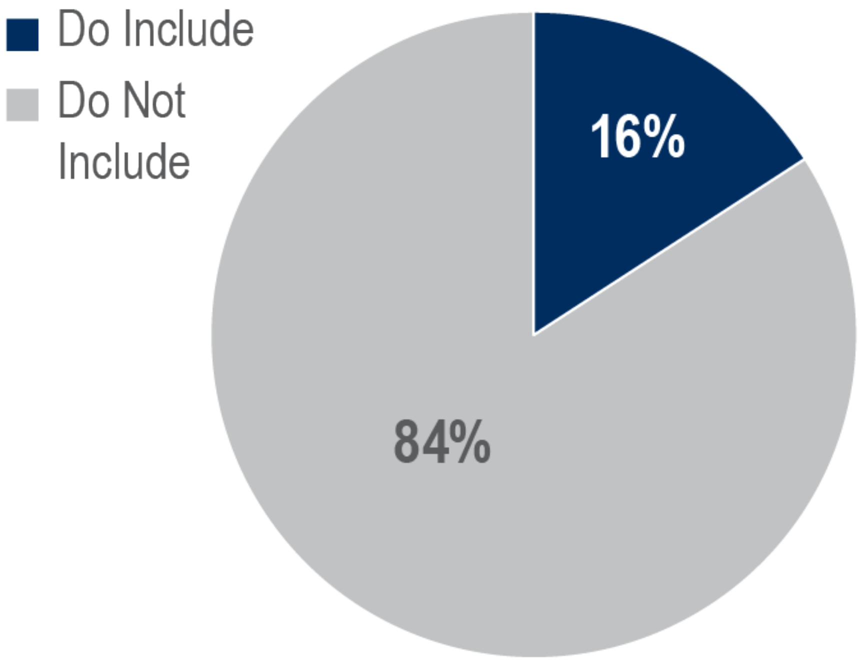
SNS: Cybersecurity Funding

Funding for Cybersecurity

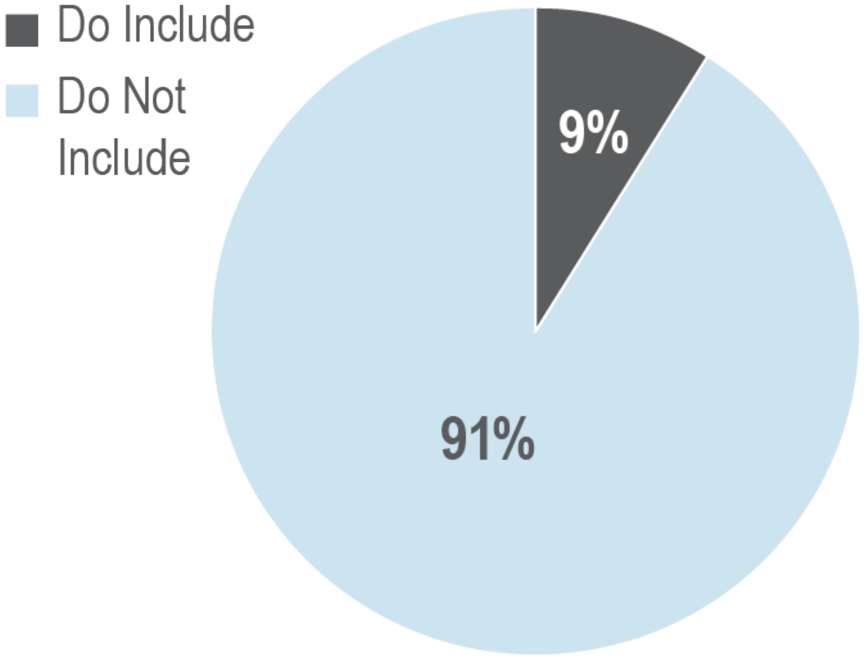


SNS: Cybersecurity Additional Insights

Cybersecurity Included as a Topic in SOPs



Cybersecurity Included in Emergency Communications Training



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 & Leadership

- Include cybersecurity representatives in governance bodies

Goal 2

Planning & Procedures

- Educate public safety agencies on cybersecurity risk mitigation
- Develop and maintain a cyber incident response plan

Goal 3

Training, Exercises, & Evaluation

- Update training and exercise programs to address cybersecurity

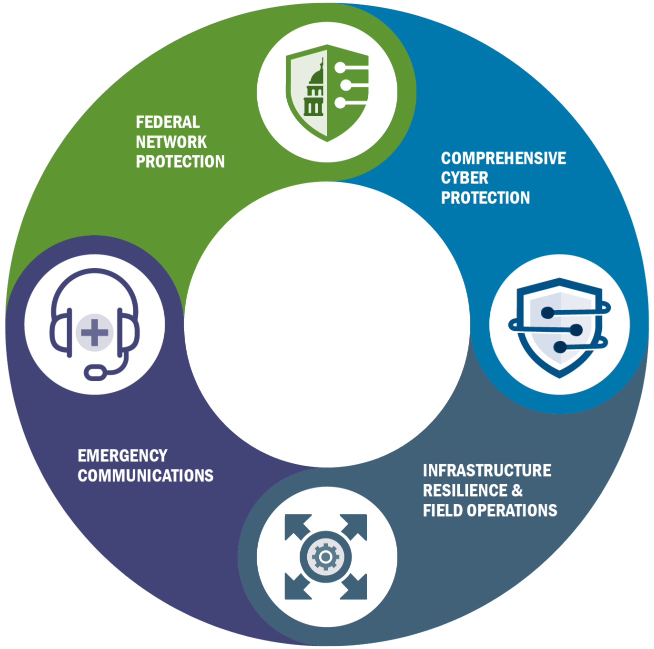
The Ransomware Threat

Cybersecurity and Infrastructure Security Agency (CISA)

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

STRENGTHEN NATIONAL RESILENCE

The Cybersecurity and Infrastructure Security Agency (CISA) is the pinnacle of national risk management for cyber and physical infrastructure

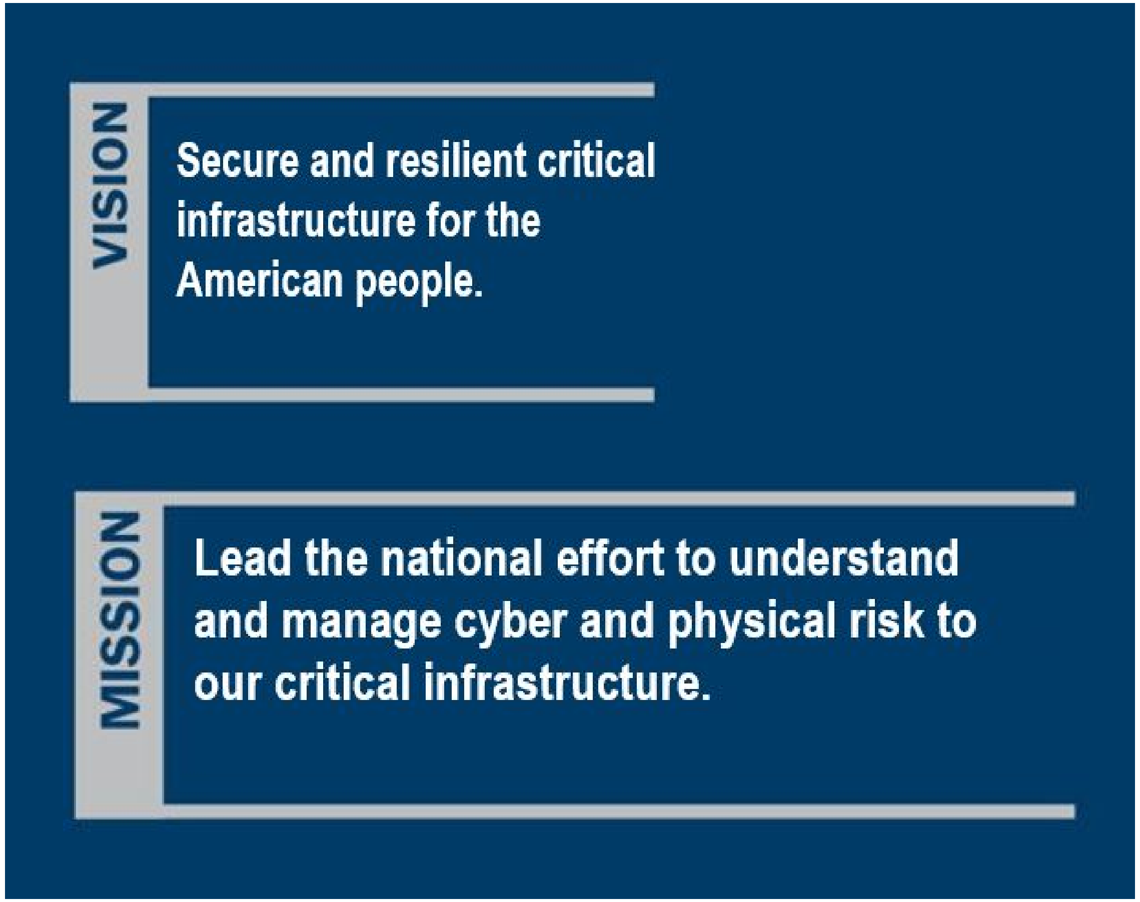


FEDERAL NETWORK PROTECTION

COMPREHENSIVE CYBER PROTECTION

INFRASTRUCTURE RESILIENCE & FIELD OPERATIONS

EMERGENCY COMMUNICATIONS



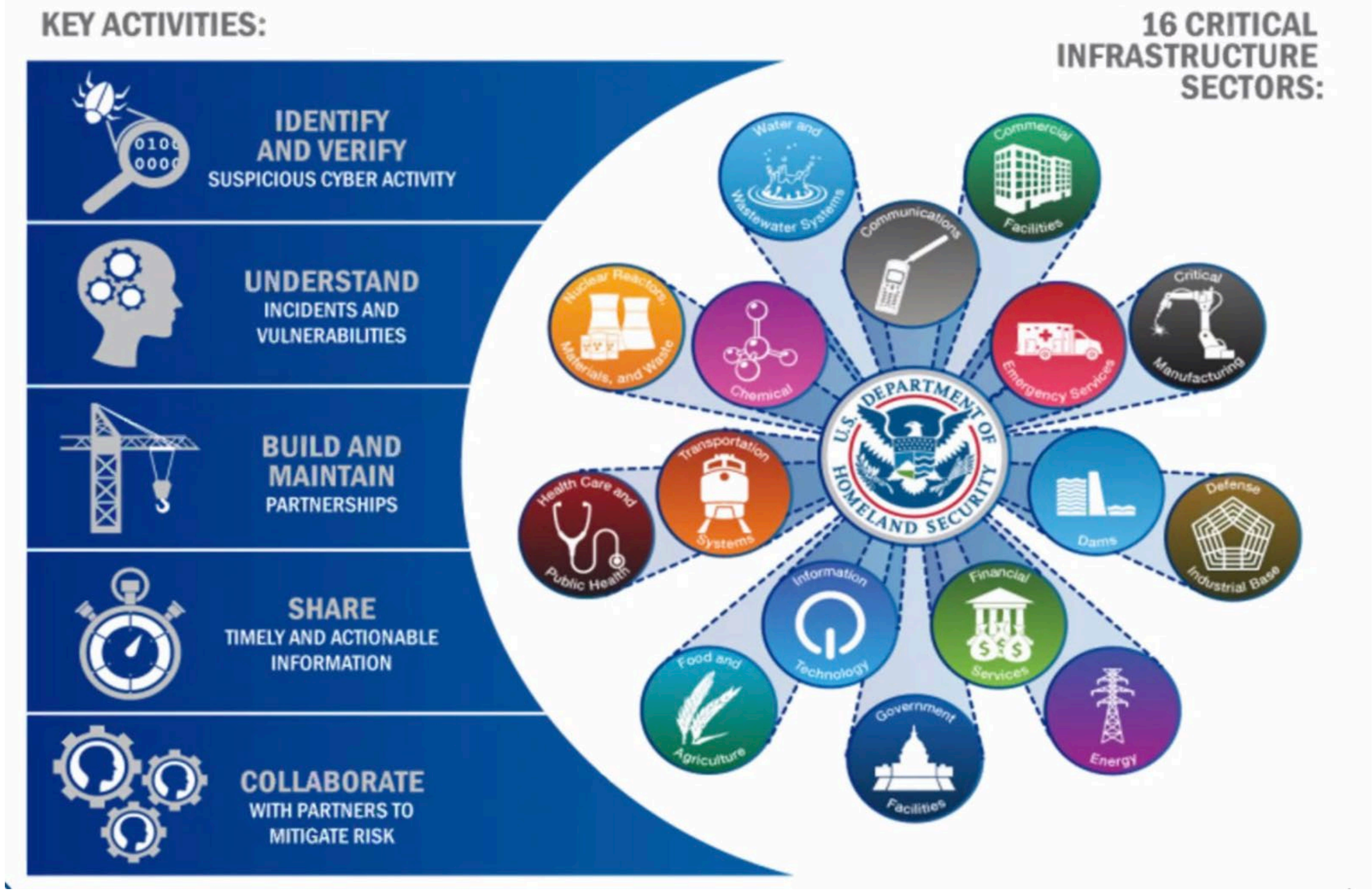
VISION

Secure and resilient critical infrastructure for the American people.

MISSION

Lead the national effort to understand and manage cyber and physical risk to our critical infrastructure.

Critical Infrastructure Focused



KEY ACTIVITIES:

IDENTIFY AND VERIFY SUSPICIOUS CYBER ACTIVITY

UNDERSTAND INCIDENTS AND VULNERABILITIES

BUILD AND MAINTAIN PARTNERSHIPS

SHARE TIMELY AND ACTIONABLE INFORMATION

COLLABORATE WITH PARTNERS TO MITIGATE RISK

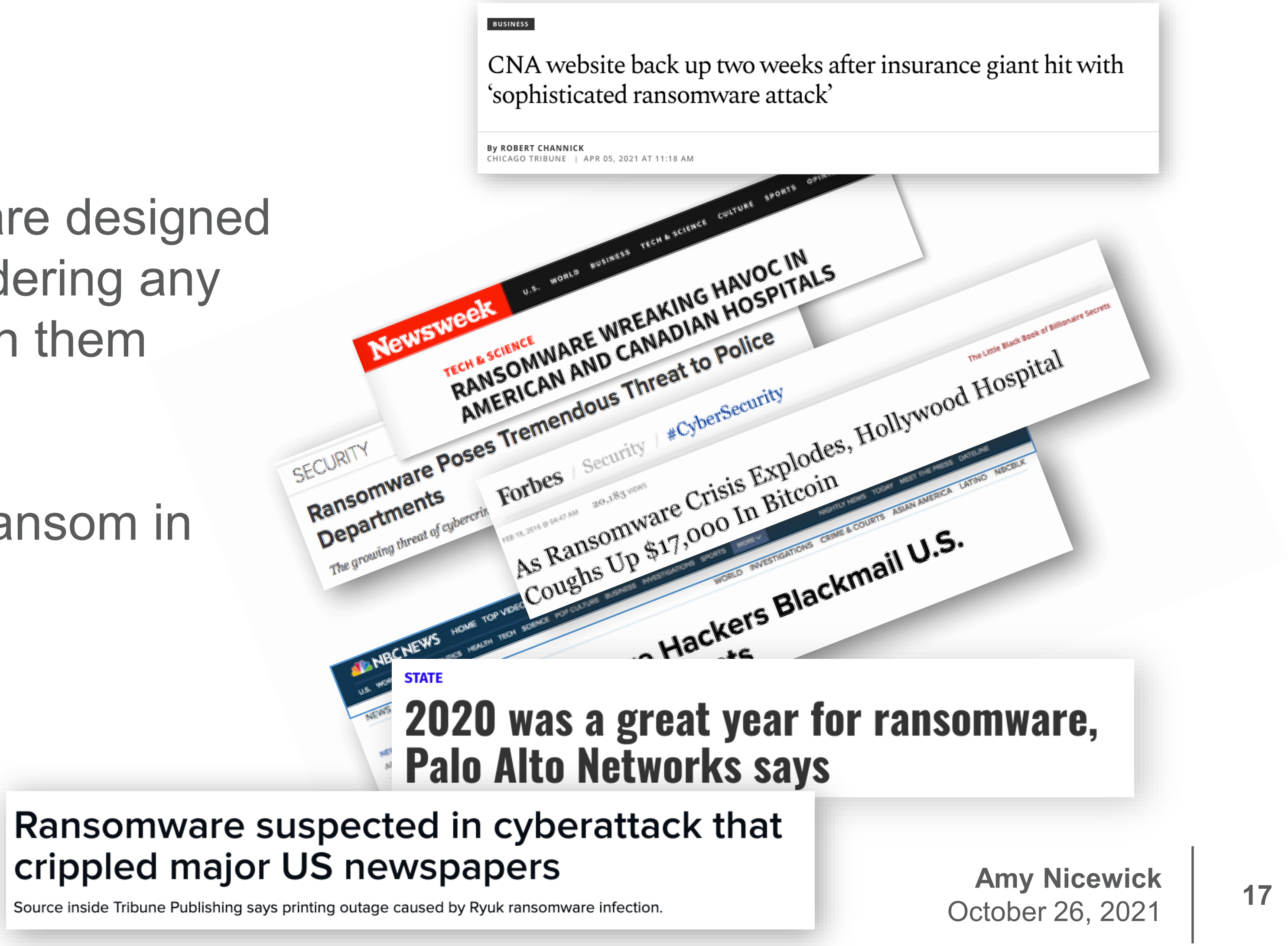
16 CRITICAL INFRASTRUCTURE SECTORS:

Beyond the Headlines: What is Ransomware?

Ransomware 101

Ransomware is a form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable.

Malicious actors then demand ransom in exchange for decryption.



BUSINESS

CNA website back up two weeks after insurance giant hit with 'sophisticated ransomware attack'

By ROBERT CHANNICK
CHICAGO TRIBUNE | APR 05, 2021 AT 11:18 AM

Newsweek

TECH & SCIENCE

RANSOMWARE WREAKING HAVOC IN AMERICAN AND CANADIAN HOSPITALS

SECURITY

Ransomware Poses Tremendous Threat to Police Departments

The growing threat of cybercri

Forbes / Security / #CyberSecurity

As Ransomware Crisis Explodes, Hollywood Hospital Coughs Up $17,000 In Bitcoin

NBC NEWS

Hackers Blackmail U.S.

STATE

2020 was a great year for ransomware, Palo Alto Networks says

Ransomware suspected in cyberattack that crippled major US newspapers

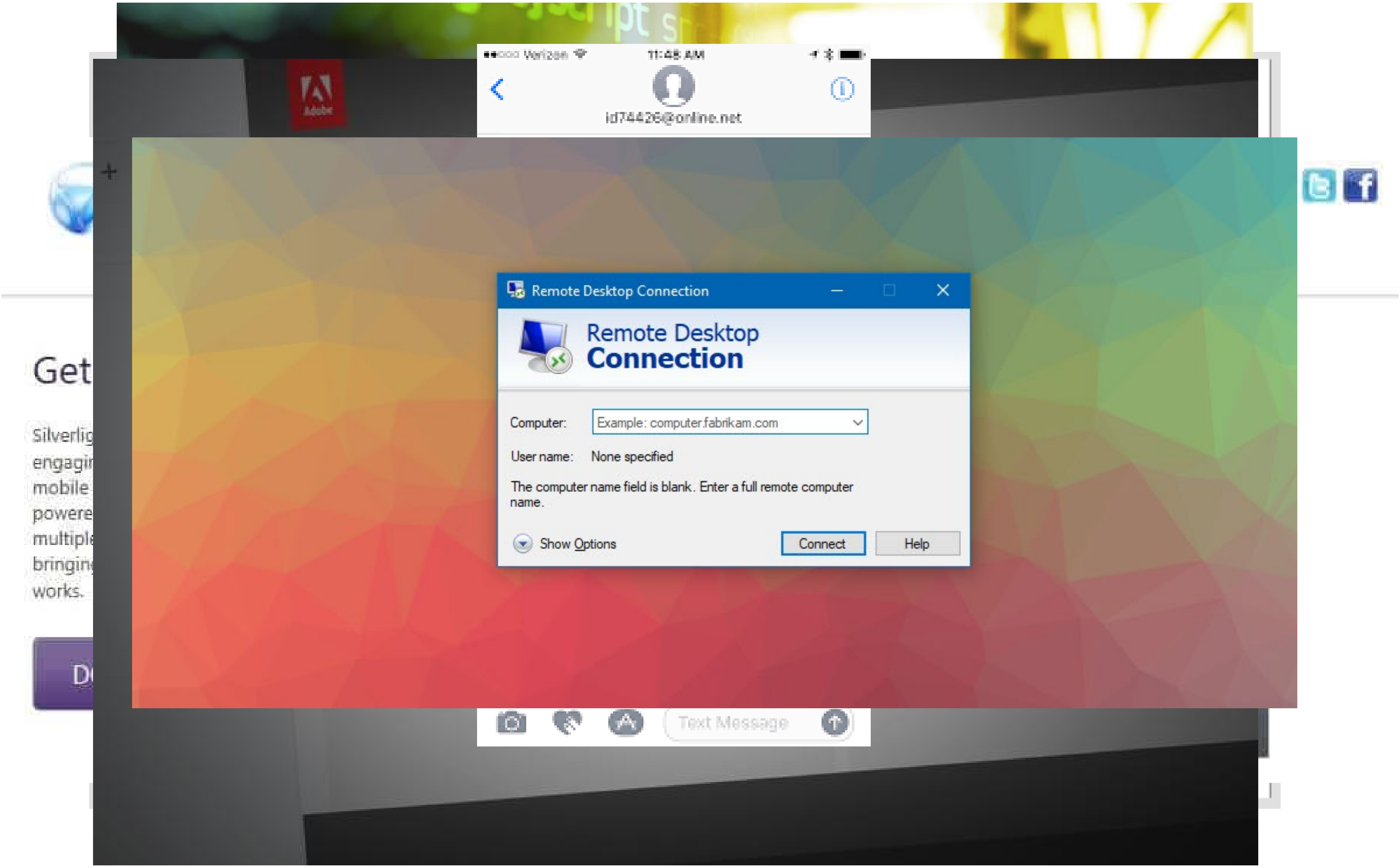
Source inside Tribune Publishing says printing outage caused by Ryuk ransomware infection.

Amy Nicewick
October 26, 2021

Methods of Infection

The following can all be vectors of infection for ransomware attacks:

- Phishing
- Compromised Websites
- Malvertising
- Exploit Kits
- Downloads
- Mobile Devices
- Brute Force via RDP



Remote Desktop Connection

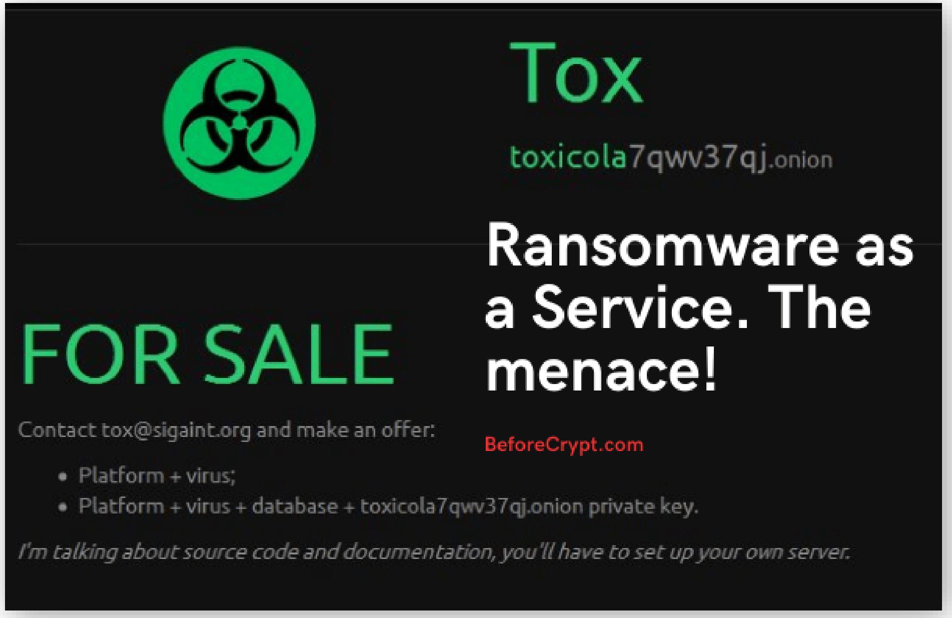
Computer: Example: computer.fabrikam.com

User name: None specified

The computer name field is blank. Enter a full remote computer name.

Trend: Ransomware-as-a-Service Model

- Ransomware families selling Ransomware-as-a-Service (RaaS) to other cybercriminals
- Popularity increases → Barriers to entry drop, becomes scalable, more efficient
- Enables relatively unskilled bad actors to access complex tools and the environment from which to run their campaigns



Tox

toxicola7qwv37qj.onion

Ransomware as a Service. The menace!

FOR SALE

Contact tox@sigaint.org and make an offer:

- Platform + virus;
- Platform + virus + database + toxicola7qwv37qj.onion private key.

I'm talking about source code and documentation, you'll have to set up your own server.

BeforeCrypt.com

- The "commoditization" of the ransomware threat: Entrepreneurial Operators, including NetWalker, Nefilim, and Sodinokibi/REvil all provide access to partners in pre-agreed profit-sharing arrangements
- Increased investment in many of the platforms themselves, upgrading their core ransomware systems to stay ahead of the good guys and evade detection

Trend: Double Extortion

- **Weaponized**: One part Ransomware, One Part Data Breach
- **Old Paradigm**: Victim's data encrypted, actor locks victim out of their own files. If victim refuses to pay the ransom, the actor destroys their files.
- **New Paradigm**:
  - Attacker exfiltrates data (e.g., large quantities of sensitive proprietary or sensitive information,) before encryption.
  - Attacker threatens to publish unless ransom paid, often will release small portions of data online.
  - If negotiation goes badly, attacker publishes all data and/or sells to a third party – putting added pressure on enterprises to meet the hackers' demands.

The Threat to Critical Infrastructure

Ransomware Campaign Overview

Ransomware Campaign Key Messages

KEEP CALM
AND
PATCH ON

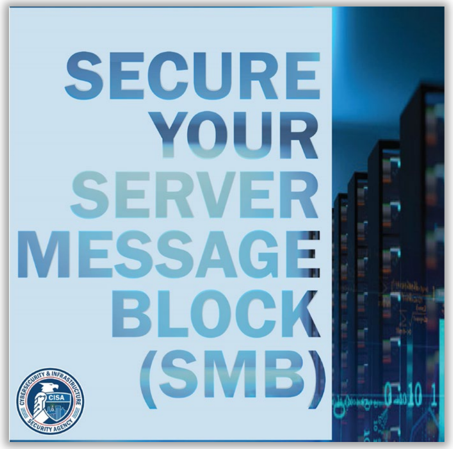
BACKING UP IS YOUR BEST BET
RANSOM!

WHEN IN DOUBT REPORT IT OUT

ALWAYS AUTHENTICATE

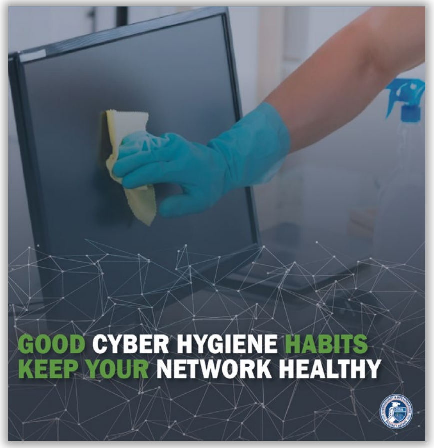
PREPARE & PRACTICE YOUR PLAN

YOUR DATA WILL BE FINE IF IT'S STORED OFFLINE...

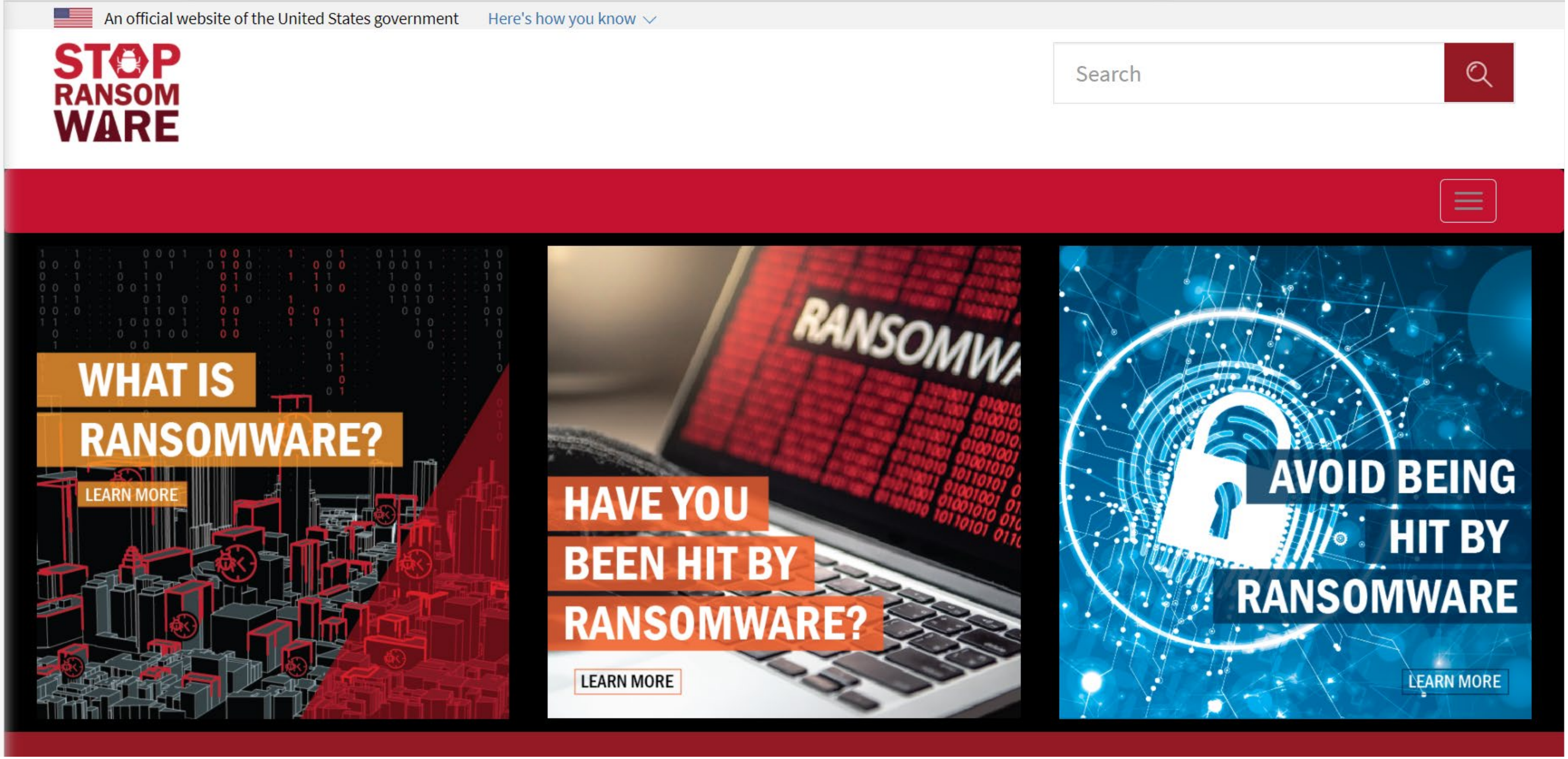


PAYING RANSOMS DOESN'T PAY OFF

RANSOMWARE REBUILD AND RECOVERY RECOMMENDATIONS



Federal Ransomware Website



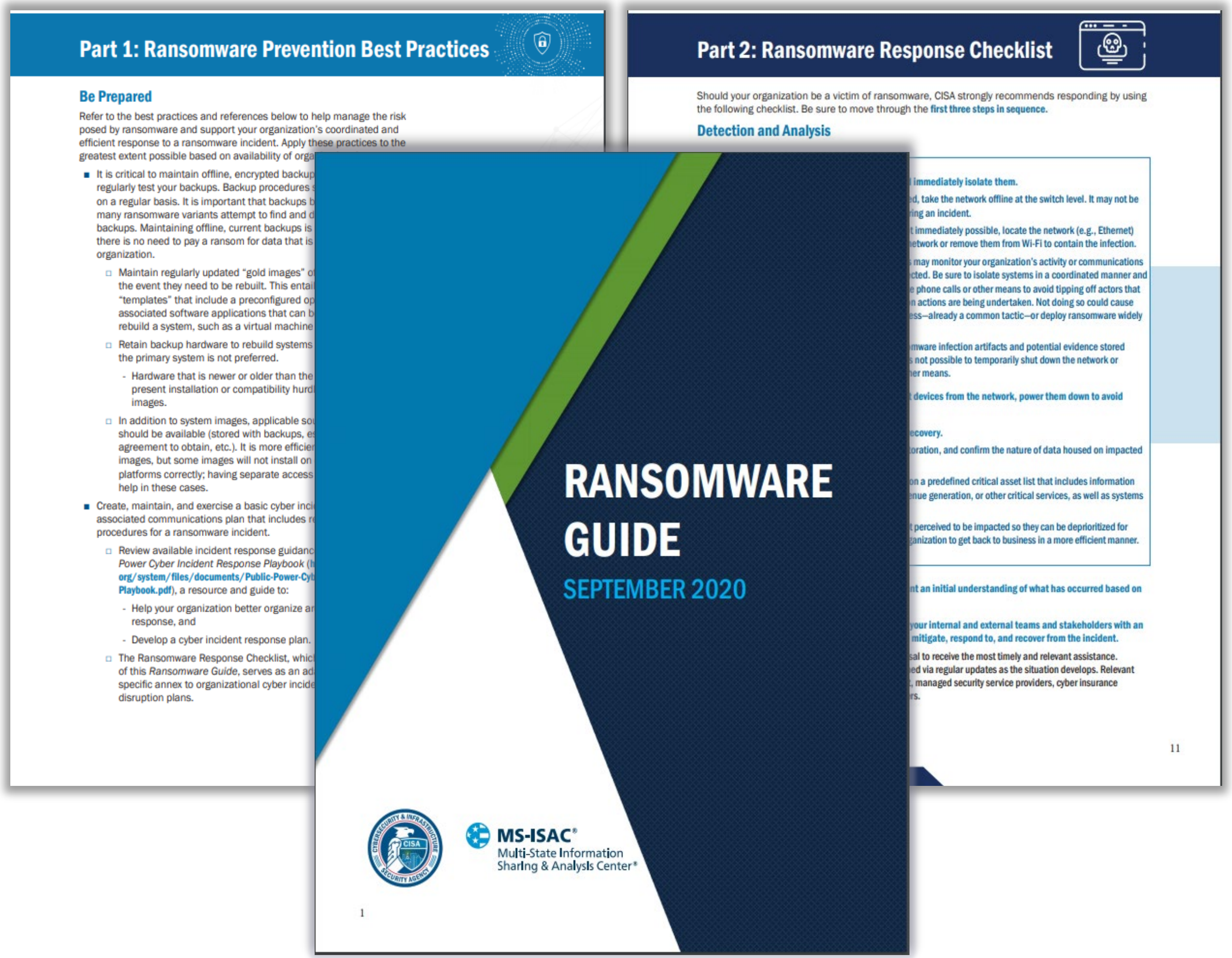
An official website of the United States government Here's how you know

Visit StopRansomware.gov today!

Ransomware Guide

Joint CISA and MS-ISAC Ransomware Guide

This Ransomware Guide includes recommendations, best practices, recommended incident response policies and procedures, cyber hygiene services, and several checklists that organizations can use to help protect against or response to ransomware attacks.



Part 1: Ransomware Prevention Best Practices

Be Prepared

Refer to the best practices and references below to help manage the risk posed by ransomware and support your organization's coordinated and efficient response to a ransomware incident. Apply these practices to the greatest extent possible based on availability of orga

- It is critical to maintain offline, encrypted backup
  regularly test your backups. Backup procedures
  on a regular basis. It is important that backups b
  many ransomware variants attempt to find and d
  backups. Maintaining offline, current backups is
  there is no need to pay a ransom for data that is
  organization.
  - □ Maintain regularly updated "gold images" o
    the event they need to be rebuilt. This entai
    "templates" that include a preconfigured op
    associated software applications that can b
    rebuild a system, such as a virtual machine
  - □ Retain backup hardware to rebuild systems
    the primary system is not preferred.
    - Hardware that is newer or older than the
      present installation or compatibility hurd
      images.
  - □ In addition to system images, applicable so
    should be available (stored with backups, e
    agreement to obtain, etc.). It is more efficie
    images, but some images will not install on
    platforms correctly; having separate access
    help in these cases.
- Create, maintain, and exercise a basic cyber inci
  associated communications plan that includes r
  procedures for a ransomware incident.
  - □ Review available incident response guidanc
    Power Cyber Incident Response Playbook (h
    **org/system/files/documents/Public-Power-Cyb
    Playbook.pdf**), a resource and guide to:
    - Help your organization better organize a
      response, and
    - Develop a cyber incident response plan.
  - □ The Ransomware Response Checklist, whic
    of this *Ransomware Guide*, serves as an ad
    specific annex to organizational cyber incide
    disruption plans.

RANSOMWARE GUIDE

SEPTEMBER 2020

MS-ISAC®
Multi-State Information
Sharing & Analysis Center®

1

Part 2: Ransomware Response Checklist

Should your organization be a victim of ransomware, CISA strongly recommends responding by using the following checklist. Be sure to move through the **first three steps in sequence.**

Detection and Analysis

immediately isolate them.
ed, take the network offline at the switch level. It may not be
ring an incident.
t immediately possible, locate the network (e.g., Ethernet)
etwork or remove them from Wi-Fi to contain the infection.
s may monitor your organization's activity or communications
cted. Be sure to isolate systems in a coordinated manner and
e phone calls or other means to avoid tipping off actors that
n actions are being undertaken. Not doing so could cause
ess—already a common tactic—or deploy ransomware widely

mware infection artifacts and potential evidence stored
s not possible to temporarily shut down the network or
er means.

devices from the network, power them down to avoid

ecovery.
oration, and confirm the nature of data housed on impacted

on a predefined critical asset list that includes information
enue generation, or other critical services, as well as systems

t perceived to be impacted so they can be deprioritized for
ganization to get back to business in a more efficient manner.

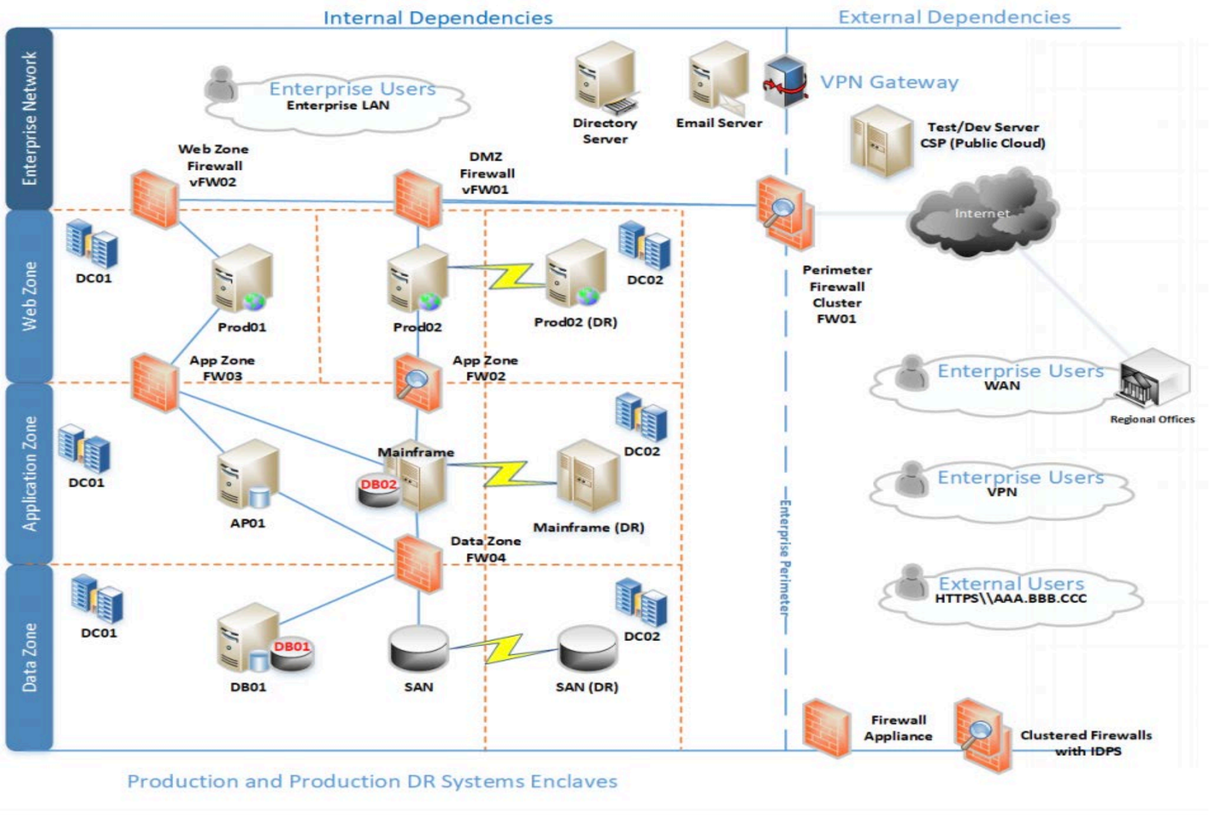
nt an initial understanding of what has occurred based on

your internal and external teams and stakeholders with an
mitigate, respond to, and recover from the incident.
sal to receive the most timely and relevant assistance.
ed via regular updates as the situation develops. Relevant
, managed security service providers, cyber insurance
rs.

11

Ransomware Guide Contents

- Best Practices to Address the Most Common Ransomware Infection Vectors:
  - Internet-Facing Vulnerabilities and Misconfigurations
  - Phishing
  - Precursor Malware Infection
  - Third-Parties and MSPs
  - General Best Practices and Hardening Guidance
- Ransomware Response Checklist
  - A ransomware-specific tear-sheet to be used as part of organization cyber incident response plan



Ransomware Guide: Select Best Practices

Maintain offline, encrypted backups of data and regularly test your backups.

Ensure antivirus and anti-malware software and signatures are up to date. Additionally, turn on automatic updates for both solutions.

Implement a cybersecurity user awareness and training program that includes guidance on identifying and reporting suspicious activity (e.g., phishing) or incidents. Conduct organization-wide phishing tests to gauge user awareness.

Employ Multifactor Authentication (MFA) for all services, particularly webmail, VPNs, and accounts that access critical systems.

These ransomware best practices and recommendations are based on operational insight from the Cybersecurity and Infrastructure Security Agency (CISA) and the Multi-State Information Sharing and Analysis Center (MS-ISAC). The audience for this guide includes information technology (IT) professionals as well as others within an organization involved in developing cyber incident response policies and procedures or coordinating cyber incident response.

Ransomware Response Checklist

Detection and Analysis

✓ Determine systems impacted, immediately isolate + triage impacted systems for restoration/recovery

✓ Engage internal/external stakeholders - help to mitigate, respond to, and recover from incident

Containment and Eradication

✓ Investigate: Take a system image and memory capture of a sample of affected devices

✓ Conduct extended analysis to identify persistence mechanisms

Recovery and Post-Incident Activity

✓ Reconnect systems, restore data from offline, encrypted backups based on critical services prioritization

✓ Document lessons learned from the incident

Executive Decision-Making Considerations

CISA encourages organizations to develop a Ransomware Playbook that provides the practices for response as well as illustrates critical points for executive leadership involvement, including how to respond. Executives will have many considerations, including:

- Recommendations from in-house Legal Counsel, Board, etc.
- The impact of maintaining manual operations without interrupting business services.
- The impact to partner systems and operations.
- Do we have Cyber Insurance coverage?
- Reputational/Brand risk exposure.
- Financial risk and legal cost/benefit analysis

! **USG strongly recommend against paying ransom**

Other CISA No-Cost Cybersecurity Resources

- **Preparedness Activities**
  - Cybersecurity Training & Exercises
  - Information Sharing & Awareness
  - Cyber Essentials

  Found at: cisa.gov/cybersecurity

  - Cybersecurity Assessments
  - NEW Ransomware Readiness Assessment (CSET®)

  Found at: cisa.gov/cyber-resource-hub

  - National Cyber Awareness System (NCAS)
  - Report Phishing
  - Alerts & Tips

  Found at: us-cert.cisa.gov

- **Response Assistance**
  - Incident coordination
  - Malware analysis
  - Cyber Threat Indicator & Defensive Measure Submission System

- **Field-based Cybersecurity Advisors (CSAs)**
  - Incident response coordination
  - Cyber assessments
  - Working group collaboration
  - Public-private advisory assistance
  - Public private partnership development

If You Are The Victim of An Attack

Victims of ransomware should report it immediately to:

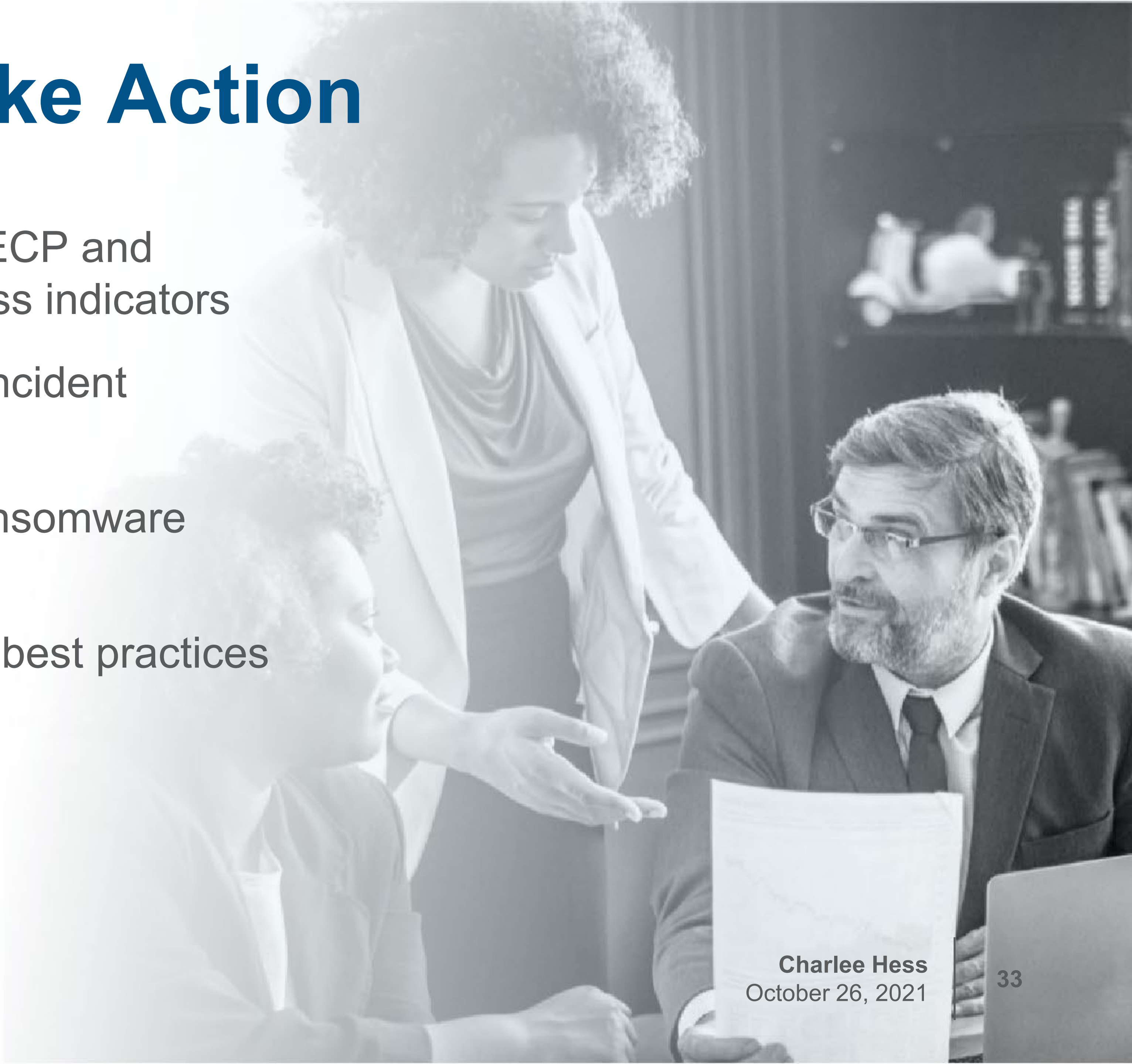
- **CISA at us-cert.cisa.gov/report;**
- **Local FBI Field Office; or**
- **Local Secret Service Field Office.**

Resources

- Cyber Risks to Public Safety Ransomware – 2020
- DHS Cybersecurity Services Catalog for State, Local, Tribal, and Territorial Governments
- National Emergency Communications Plan
- SAFECOM Nationwide Survey Results
- Ransomware Guide
- Stop Ransomware Website

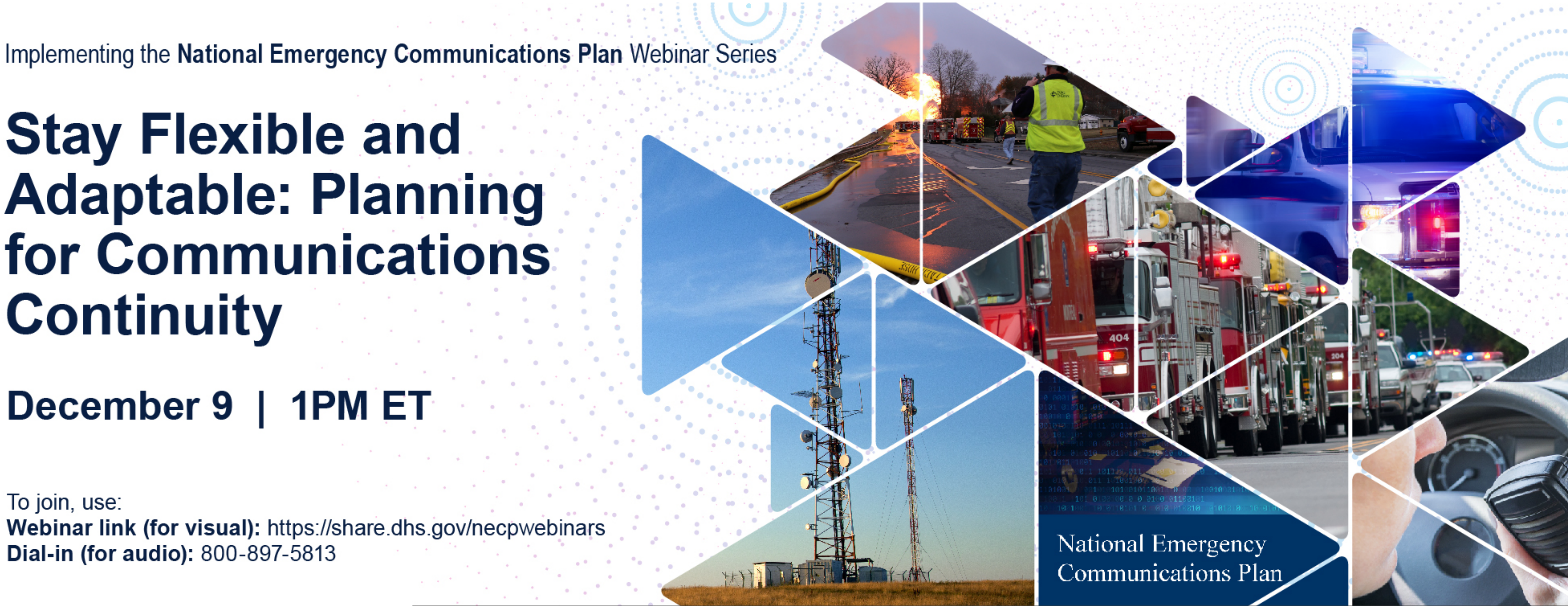
How You Can Take Action

- Take steps to implement the NECP and achieve its cybersecurity success indicators
- Develop and maintain a cyber incident response plan
- Become familiar with CISA’s ransomware resources
- Implement Ransomware Guide best practices



Questions?

Upcoming Webinars



Implementing the **National Emergency Communications Plan** Webinar Series

Stay Flexible and Adaptable: Planning for Communications Continuity

December 9 | 1PM ET

To join, use:
Webinar link (for visual): https://share.dhs.gov/necpwebinars
Dial-in (for audio): 800-897-5813

National Emergency Communications Plan

For more information:
www.cisa.gov
NECP@cisa.dhs.gov

CYBERSECURITY & INFRASTRUCTURE

CISA

SECURITY AGENCY