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

- Impact: 37%
- No Impact: 63%

Factors that Affect Ability to Communicate: Cybersecurity Disruption or Breach

- Impact: 43%
- No Impact: 57%
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

- Risk Assessment (Preventative): 34%
- Incident Response Plans, Policies, and Capabilities: 20%
- Coordinated Response and Restoration Activities with Internal/External Parties: 10%
- Incident Response Team (IRT): 6%
- None of the Above: 46%
SNS: Cybersecurity Funding

Funding for Cybersecurity

- There is no funding for this item: 56%
- There is funding, but it is insufficient to meet needs: 26%
- There is funding, and it is sufficient for all needs: 15%
- Funding is sufficient and has been identified to address needs beyond the current budget cycle: 3%
SNS: Cybersecurity Additional Insights

Cybersecurity Included as a Topic in SOPs

- Do Include: 16%
- Do Not Include: 84%

Cybersecurity Included in Emergency Communications Training

- Do Include: 9%
- Do Not Include: 91%
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
STRENGTHEN NATIONAL RESILIENCE

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

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:
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.
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
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
- 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
- When in doubt report it out
- Always authenticate
- Prepare & practice your plan
- Your data will be fine if it's stored offline
- Secure your server message block (SMB)
- Paying ransoms doesn't pay off
- Ransomware rebuild and recovery recommendations
- Good cyber hygiene habits keep your network healthy
Federal Ransomware Website

Visit StopRansomware.gov today!
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.
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
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.
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

Charlee Hess
October 26, 2021
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
For more information:
www.cisa.gov
NECP@cisa.dhs.gov