IT Security | Supply Chain | OT Security | Insider Threat | Physical Security | Interoperable Communications

Cybersecurity:

Emergency Communications by the Numbers

OVERVIEW

Cybersecurity is a shared mission across all levels of government, the private sector, nongovernmental organizations, and the public. Organizations can enhance their cybersecurity posture through proactive risk assessments, network and software monitoring, enhanced identity authentication, and cyber incident response planning and exercises. Organizations can achieve the successful implementation of these cybersecurity measures by developing and updating standard operating procedures (SOP) that address cybersecurity. In addition, keeping training up to date with the latest physical and cyber security practices is a key component to maintaining resilient operations. According to results from the SAFECOM Nationwide Survey (SNS)[1], nearly half of public safety organizations have not taken measures to prevent or mitigate the impact of cybersecurity incidents. This document discusses cybersecurity gaps identified by the SNS as well as the benefits of enhanced cybersecurity preparedness. It also describes actions in the National Emergency Communications Plan (NECP) that organizations can take to improve their cybersecurity posture.

Gaps in Cybersecurity Identified by the SNS

31 percent of public safety organizations indicated they have not adopted any of the cybersecurity elements included in the SNS

Only **21 percent** of public safety organizations indicated cybersecurity is included in their SOPs

Only **15 percent** of public safety organizations indicated cybersecurity is included in personnel training

BENEFITS OF IMPROVED CYBERSECURITY PRACTICES

- Risk assessment
- Mitigation strategies
- Mitigation evaluation, implementation, and testing
- Continuous monitoring
- Threat/vulnerability identification
- Incident Response Teams
- Incident response plans, policies, and capabilities
- Agreements with U.S. Computer Emergency Readiness Team
- Coordinated response and restoration activities with internal and external parties
- Single factor authentication
- Multi-factor authentication

The SNS collected information regarding the adoption of 11 cybersecurity elements by public safety organizations.

Findings revealed that organizations that reported adopting 10 or more cybersecurity elements were:

44 percent more likely to report little or no cybersecurity impact on emergency response providers' ability to communicate in the most recent period covered by the SNS from 2011 to 2016

1.5 times more likely to report personnel are adequately trained to achieve communications operability and continuity in out-of-the-ordinary situations

Between **2.5 and 3.5 times more likely** to report significant strengthening in emergency communications operability, continuity, and interoperability in day-to-day situations, and between **3.5 and 4 times more likely** to report significant strengthening in out-of-the-ordinary situations

[1] The SNS is a nationwide data collection effort to obtain actionable and critical data that drives our nation's emergency communications policies, programs, and funding. The survey is conducted every five years.

CYBERSECURITY IN STANDARD OPERATING PROCEDURES AND TRAINING

SNS data also shows that respondents who indicated that cybersecurity is included in their SOPs and training are more likely to report a better cybersecurity posture.

Public safety organizations are **82-83 percent more likely** to report cybersecurity incidents had little or no impact on their ability to communicate when cybersecurity is included in SOPs and training

CYBERSECURITY IN THE NATIONAL EMERGENCY COMMUNICATIONS PLAN

The NECP includes recommended actions for cybersecurity preparedness. By incorporating these measures, public safety organizations can improve their cybersecurity posture:

Goal 1: Governance
✓ Include information management, network infrastructure, and cybersecurity representatives in emergency communications governance groups through membership or formalized coordination
Goal 2: Planning and Procedures
✓ Incorporate risk management strategies into plans for continuity and recovery of critical communications
Goal 3: Evaluations, Training, and Exercises
✓ Develop or update training and exercise programs to address cybersecurity
Goal 4: Communications Coordination
✓ Develop and regularly update National Incident Management System-aligned standard operating procedures to facilitate the integration of cybersecurity best practices
Goal 6: Cybersecurity
✓ Implement the National Institute of Standards and Technology (NIST) Cybersecurity Framework[2]
✓ Perform a Cyber Resilience Review[3]
✓ Leverage ongoing NIST work to plan for setting, testing, and maintaining cyber minimum standards to assist cybersecurity-eligible grant programs in prioritizing and distributing necessary funding to public safety

RESOURCES FOR IMPROVING CYBERSECURITY

CISA Planning and Policy Support

- National Emergency Communications Plan
- SAFECOM Nationwide Survey

CISA Cybersecurity Support

- CISA Alerts & Tips
- CISA Central
- CISA Cyber Resource Hub
- Communications and Cyber Resiliency
  - Cyber Resiliency Resources for Public Safety Fact Sheet
  - Public Safety Communications and Cyber Resiliency Toolkit

CISA Cybersecurity Support, continued

- Cybersecurity for 911 and NG911 Systems
- Cybersecurity Performance Goals
- Interoperable Communications Technical Assistance Program: Service Offerings Guide

Additional Cybersecurity Support

- Department of Homeland Security Cybersecurity Services Catalog
- NIST Cybersecurity Framework

For more information on the SNS or NECP, contact necp@cisa.dhs.gov

[2] The NIST Cybersecurity Framework is a flexible, risk-based approach to improving the security of critical infrastructure.

[3] A Cyber Resilience Review is a no-cost, voluntary assessment available from CISA to evaluate an organization's operational resilience and cybersecurity practices.