IMPLEMENTING THE NECP WEBINARS

BUILDING RESILIENCE: THE POWER OF MULTIFACTOR AUTHENTICATION IN PUBLIC SAFETY COMMUNICATIONS

APRIL 24, 2024

Anais Azoulay
April 24, 2024

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

Anais Azoulay
IT Cybersecurity Specialist, Emergency Communications Division
Cybersecurity and Infrastructure Security Agency

Bryce Bailey
IT Cybersecurity Specialist, Cybersecurity Division
Cybersecurity and Infrastructure Security Agency

Savanah Courtney
Cyber Risk Analyst, Cybersecurity Division
Cybersecurity and Infrastructure Security Agency

Chetrice Romero
Cybersecurity Advisor, Indiana
Cybersecurity and Infrastructure Security Agency

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

Mandate

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

Nation's Strategic Plan

The NECP is the nation's strategic plan to strengthen and enhance emergency communications capabilities

Mission

To ensure the emergency response community drives toward a commonly defined end-state for communications

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 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

75%

of local public safety organizations **have identified cyberattacks perpetrated against** their organization

20%

of local public safety organizations **have identified unauthorized systems access and/or credential attacks against** their agency

SNS: Cybersecurity Posture

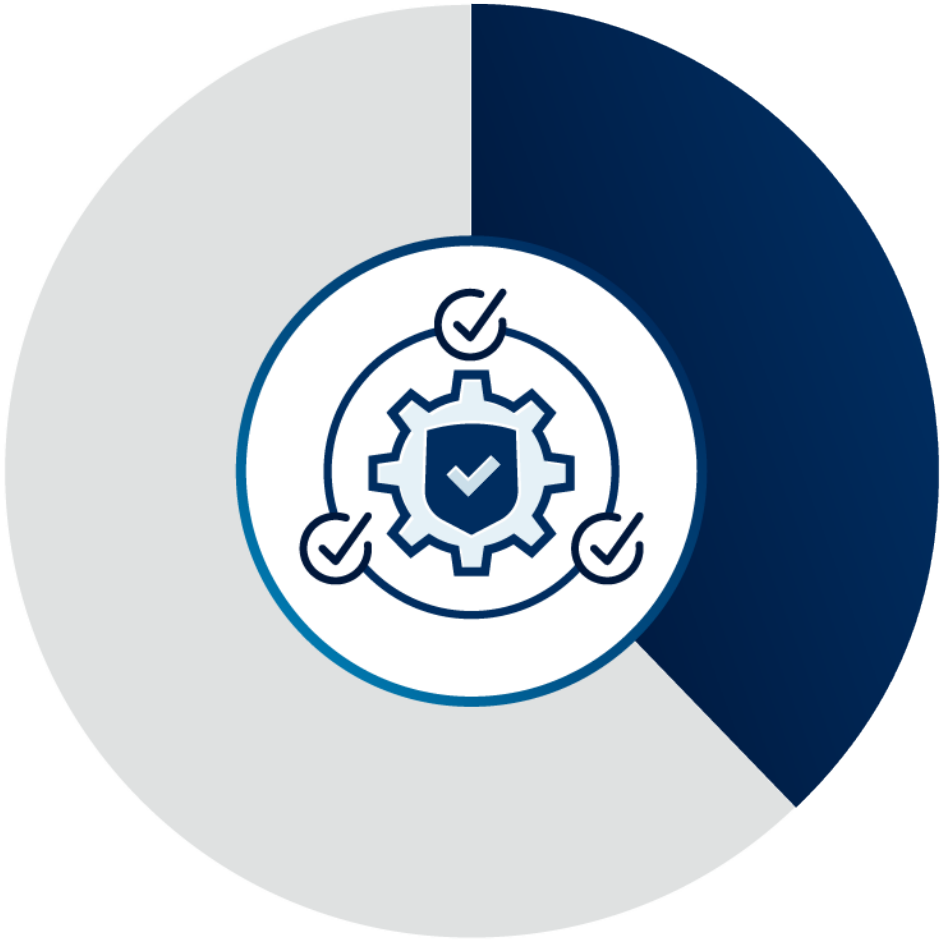
41%

of local public safety organizations **do not engage in cybersecurity planning or implementation**

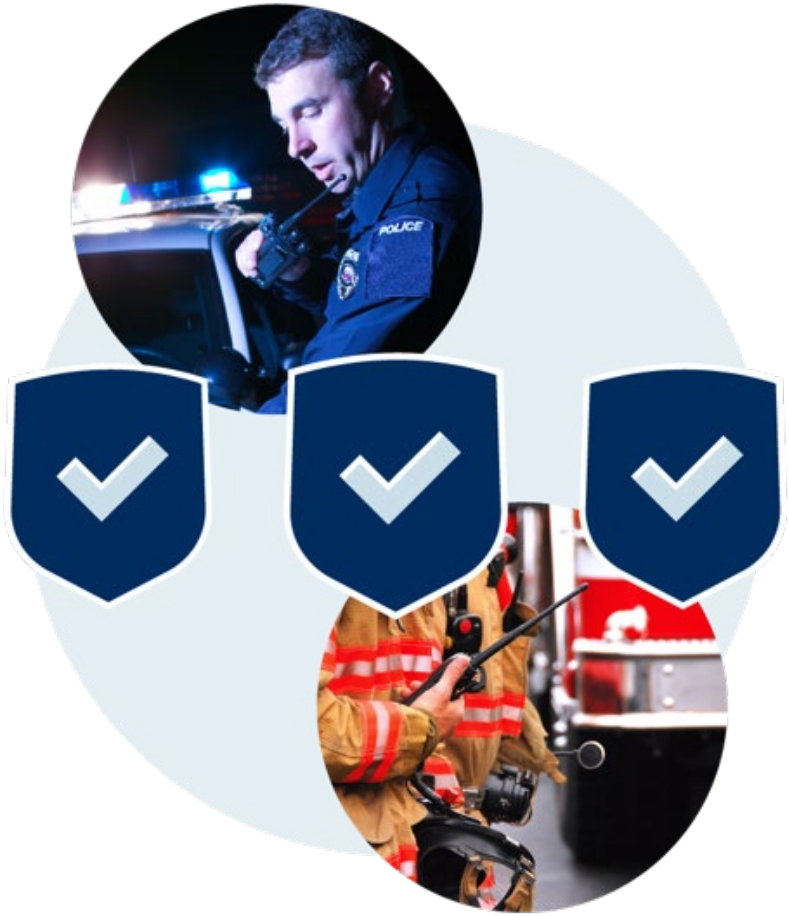
SNS: Multifactor Authentication

38%

of local public safety organizations **have implemented MFA** in their agency



SNS: Multifactor Authentication



Local public safety organizations **with MFA are almost three times as likely to feel confident** in their ability to detect and respond to cybersecurity threats, compared to their counterparts without MFA

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

CYBER RISK, MFA AND IMPLICATIONS TO EMERGENCY SERVICES

Overview

What is Cyber Risk?

Threats to the Emergency Services Sector

Case Study: Dallas 2023

Lessons learned

Current Conditions: Vulnerabilities in the ESS

How can MFA protect your organization?

What is Cybersecurity Risk?

Cyber Risk: The likelihood that any specific threat will exploit a specific vulnerability that causes harm as a result of the unauthorized disclosure, modification, or destruction of information or loss of information or system availability.

Threat

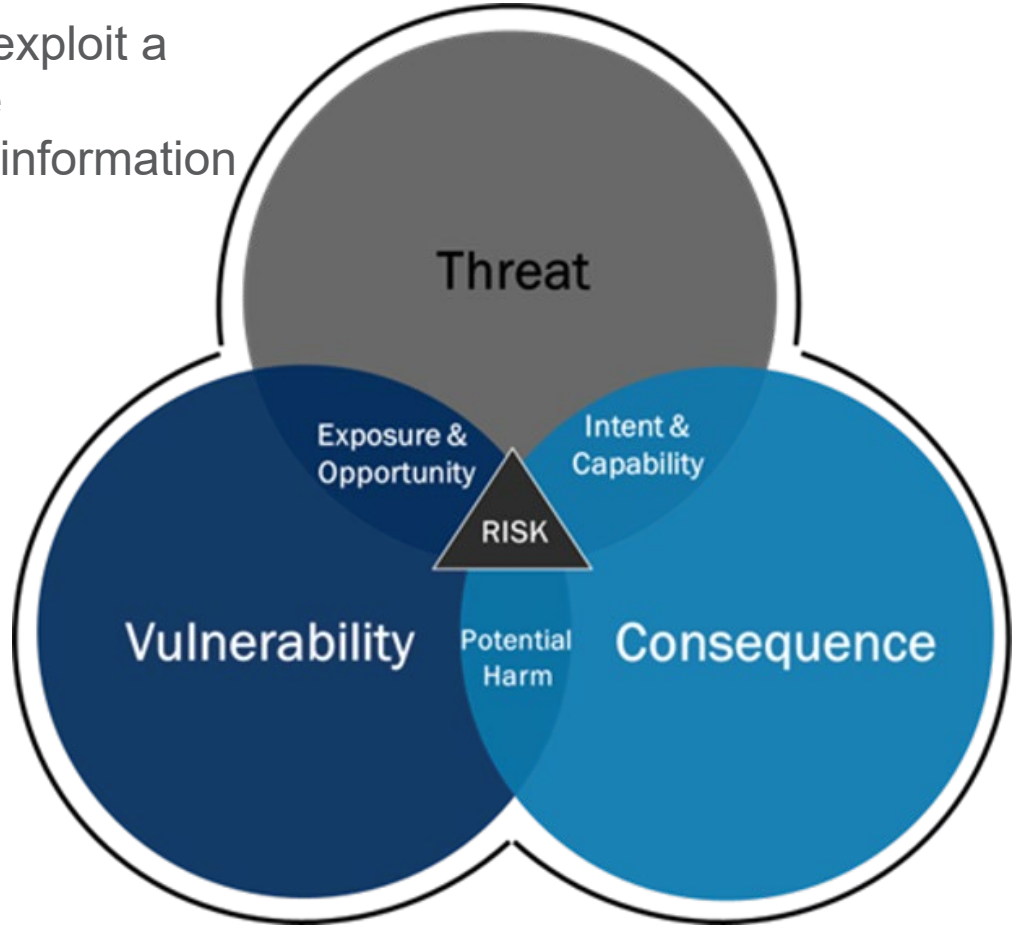
- People, programs, hardware, or systems with the intent, capability, and opportunity to exploit vulnerabilities

Vulnerability

- A weakness in the information (IT) or operational (OT) technology infrastructure or any other aspect of an organization.

Consequence

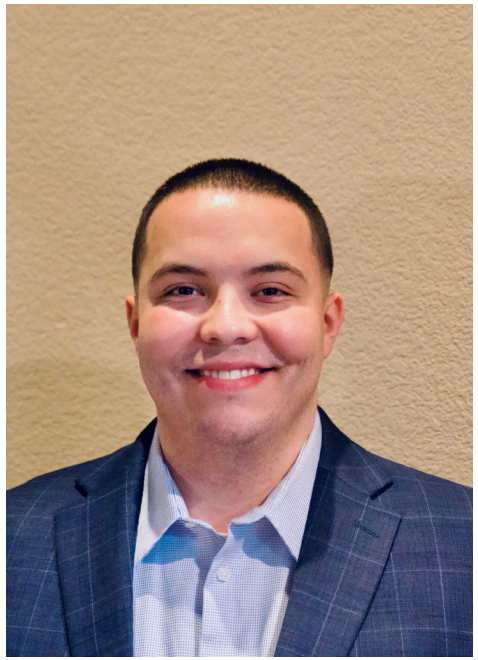
- Effect of an event, incident, or occurrence



Team

Savanah Courtney

Cyber Risk Analyst



Bryce Bailey

IT Cybersecurity Specialist

Case Study: Dallas 2023

Due to the Royal Ransomware Attack:

- Dispatchers had to handwrite information and relay over congested radio networks
- Firefighters and police officers impacted and could not do their jobs
- Other dependency issues

Briefing Overview

DATA SOURCE(S)

Analyzed voluntary-participating stakeholders:

CISA Vulnerability Scanning (VS)

Open Source Reporting & Data

Industry Reports

TIMEFRAME

Period of analysis is from January 1, 2024 to April 11, 2024.

ESS entities enrolled in CISA VS prior to April 1, 2024 are represented in this briefing

CAVEAT

The entities depicted in this briefing may not be considered statistically representative of the U.S. ESS Sector

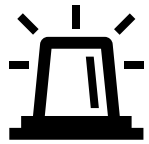
However, all entities are encouraged to adopt CISA's recommendations and best practices, as applicable.

The resulting analysis uses the MITRE ATT&CK® for Enterprise framework, Version 13.1.

Known Threats to the Sector

The Emergency Services Sector (ESS) entities operate with vulnerable, internet-accessible products, applications, and software that are **actively exploited**.

188 total entities


Analysis is derived from the cybersecurity vulnerability information received through the CISA Cyber Hygiene (CyHy) Vulnerability Scanning (VS) and Web Application Scanning (WAS) services as of April 2024.

Known Exploited Vulnerabilities (KEVs)

Vendor	CVE	Ransomware
PHP	CVE-2019-11043	Known
Apache	CVE-2020-1938	
Cisco	CVE-2020-3452	
Cisco	CVE-2020-3580	
Apache	CVE-2021-40438	
Ivanti	CVE-2024-21887	

The exposed KEVs could allow for credential theft in many cases (XXS/SSRF), where MFA could add complexity for an attacker to use the stolen passwords. Other KEVs exposed below:

Remote Code Execution KEVs:
- CVE-2019-11043 (PHP)

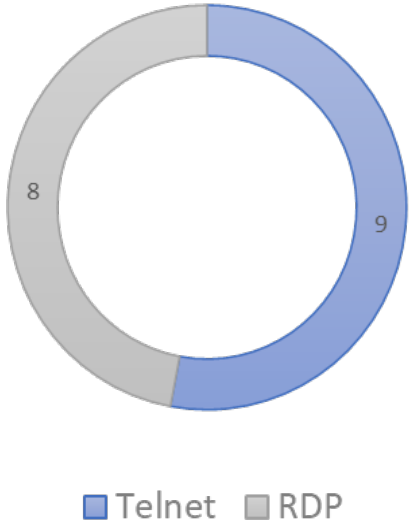
Privilege Management
- CVE-2020-1938 (Apache Tomcat)

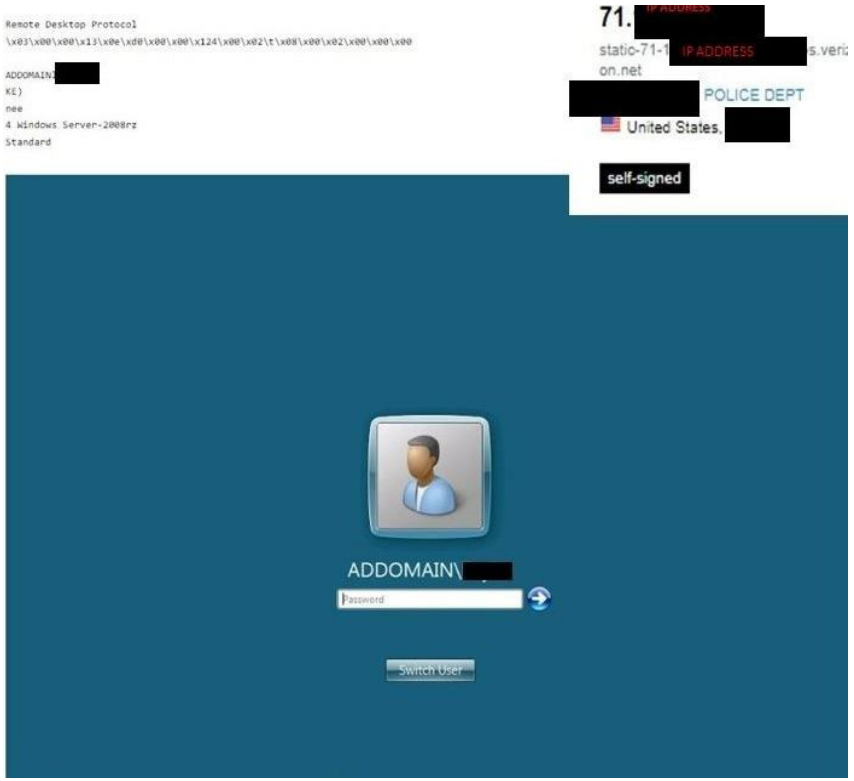
Remote Access and MFA

Exposed and Vulnerable Services: ESS entities Exposed Internet Accessible Services, based on CISA VS RDP, NetBIOS, SMB, and Telnet are high risk of compromise.

CISA also has seen remote management interfaces for security software and VPN accessible via the internet. Stolen credentials and default credentials are often used to access these interfaces.

Instances of Remote Services:



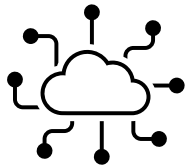


Above, open-source data from a Shodan search displays open RDP on an administrator's account; this account belongs to a police department using an OS no longer supported by Microsoft.

Email Weaknesses & Unsupported OS

Many ESS domains have Email Security Weaknesses

- Inadequate Domain-Based Message Authentication, Reporting and Conformance (DMARC) policies
- This can lead to email spoofing
- Less-than ideal filtering of spam or emails from malicious actors
- Independent email services off the back of city domains



CISA scanning data shows 34 different unsupported products/software

- Microsoft Windows from 2008 and earlier
- Free BSD

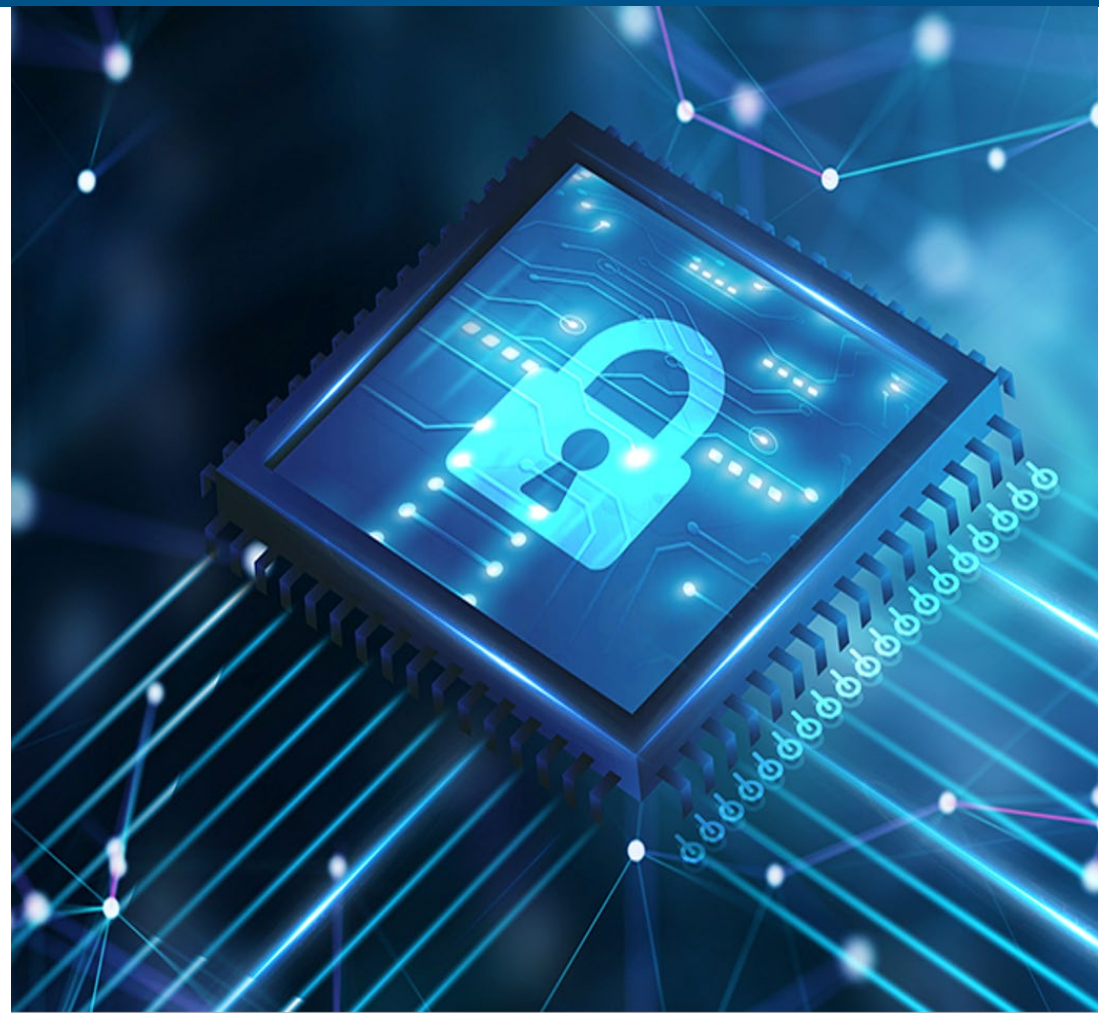
Outdated Exchange servers were a possible entry point for the DC Metropolitan Police Department incident

Ransomware Hackers Claim To Leak 250GB Of Washington, D.C., Police Data After Cops Don't Pay $4 Million Ransom (forbes.com)

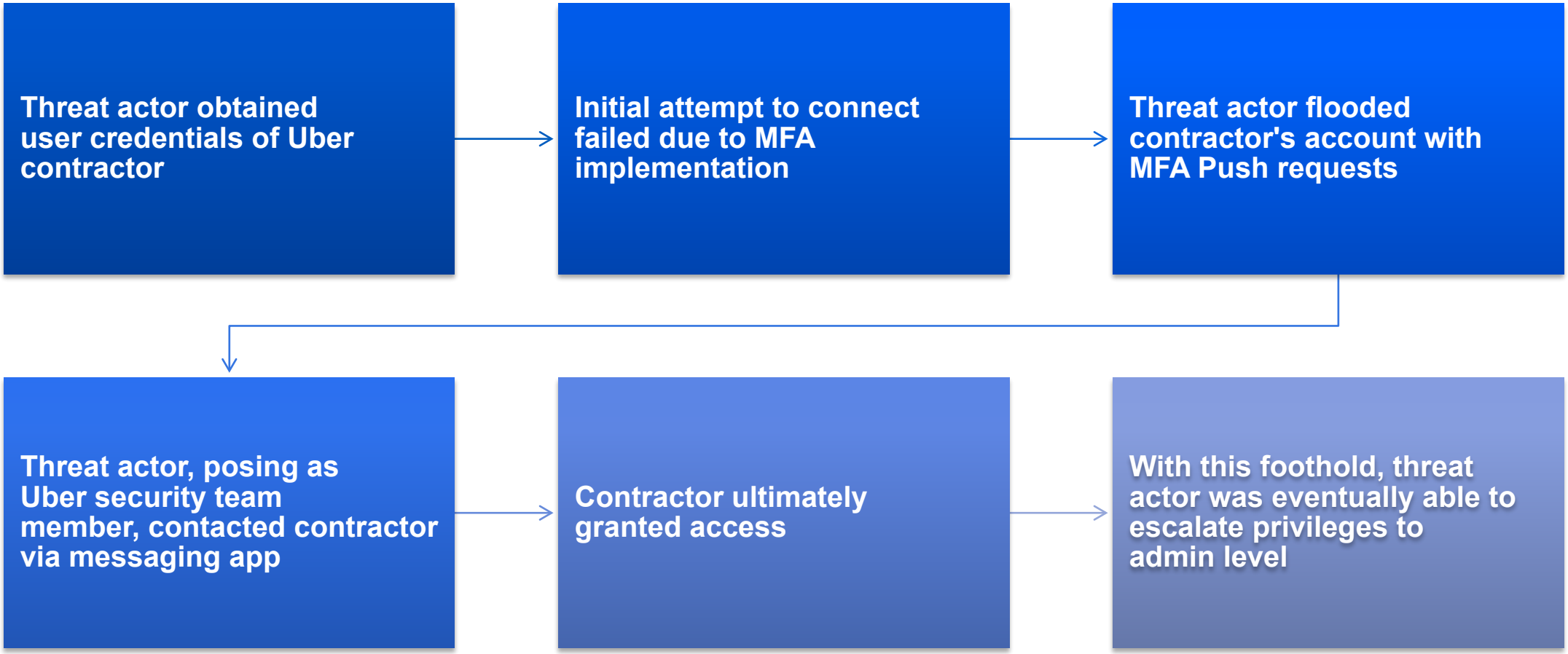
So what?

Make it hard for the adversary.

Prevent threat actors from using stolen credentials.
Control accesses.
Dodge Insider threats.
Protect against remote attacks.



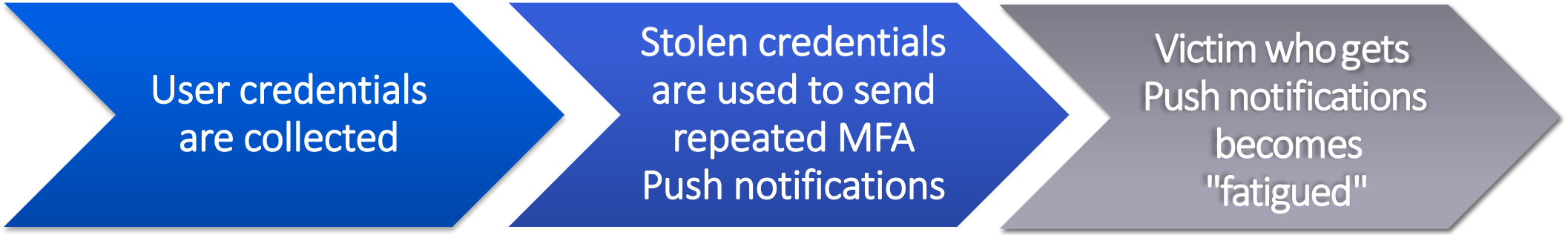
Case Study: Uber September 2022



MFA Fatigue Attacks

Social Engineering Attack

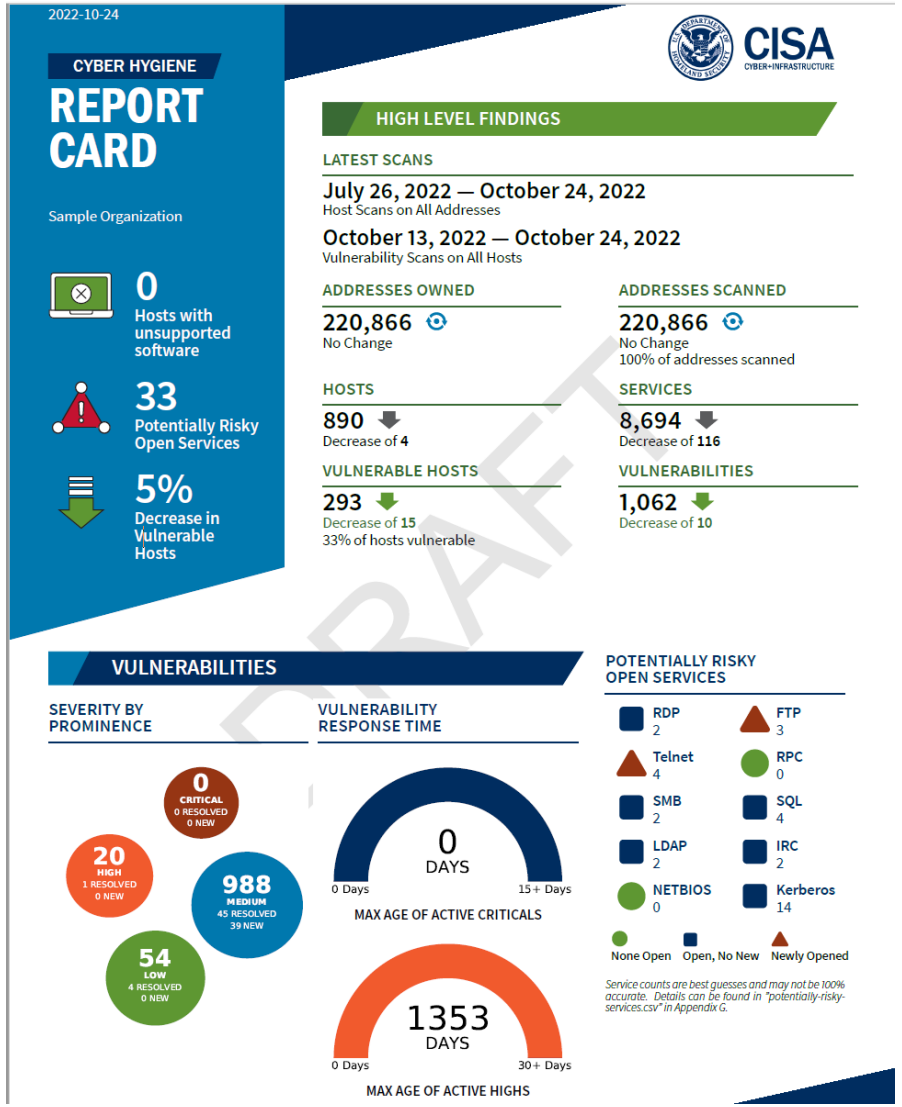
- Not particularly high-tech
- Requires attacker to already have target username and password
- Attacks weakest link in cybersecurity – **humans**
- Depends on targets' lack of training and understanding of attack vectors



CISA Vulnerability Scanning Sample Report

Exposure Factor Summary

Severity Summary



Risky Services Summary

Cybersecurity Division | Vulnerability Management

Cyber Hygiene Services

https://www.cisa.gov/cyber-hygiene-services

vulnerability@cisa.dhs.gov

CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY

Who We Are

The Cybersecurity and Infrastructure Security Agency (CISA) is the Nation's risk advisor, working with partners to defend against today's threats and collaborating to build more secure and resilient infrastructure for the future

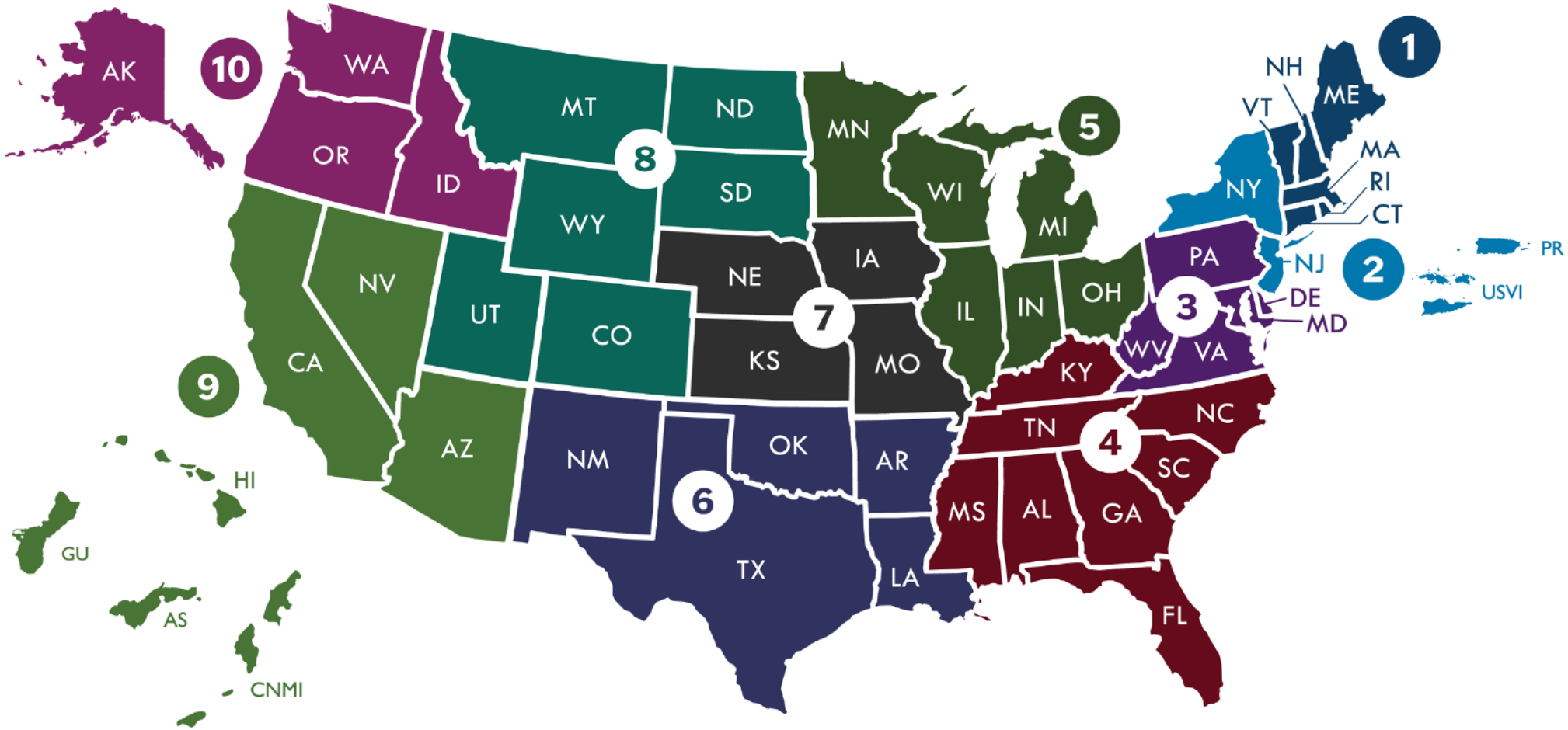
What We Do

To provide direct coordination, outreach, and regional support and assistance in the protection of cyber components essential to the Nation's Critical Infrastructure.

- **Assess**: Evaluate critical infrastructure cyber risk
- **Promote**: Encourage best practices and risk mitigation strategies
- **Build**: Initiate, develop capacity, & support cyber communities
- **Educate**: Inform and raise awareness
- **Listen**: Collect stakeholder requirements
- **Coordinate**: Bring together incident support and lessons learned

CISA Regions

- 1 Boston, MA
- 2 New York, NY
- 3 Philadelphia, PA
- 4 Atlanta, GA
- 5 Chicago, IL
- 6 Dallas, TX
- 7 Kansas City, MO
- 8 Denver, CO
- 9 Oakland, CA
- 10 Seattle, WA



Cisa.gov/regions

REDUCE YOUR CYBER RISK

Password Management!

Are Strong Passwords Enough?

Why Enable MFA

review, to evaluate the security performance of various MFA methods in a largedataset of Microsoft Azure Active Directory users exhibiting suspicious activity. Our findings reveal that MFA implementation offers outstanding protection, with over 99.99% of MFA-enabled accounts remaining secure during the investigation period. Moreover, MFA reduces the risk of compromise by 99.22% across the entire population and by 98.56% in cases of leaked credentials. We further demonstrate that dedicated MFA applications, such as Microsoft Authenticator,

Microsoft

How effective is multifactor authentication at deterring cyberattacks?

Lucas Augusto Meyer
AI for Good Lab

Sergio Romero
Identity Security

Gabriele Bertoli
Identity Security

Tom Burt
Customer Security & Trust

Alex Weinert
Identity Security

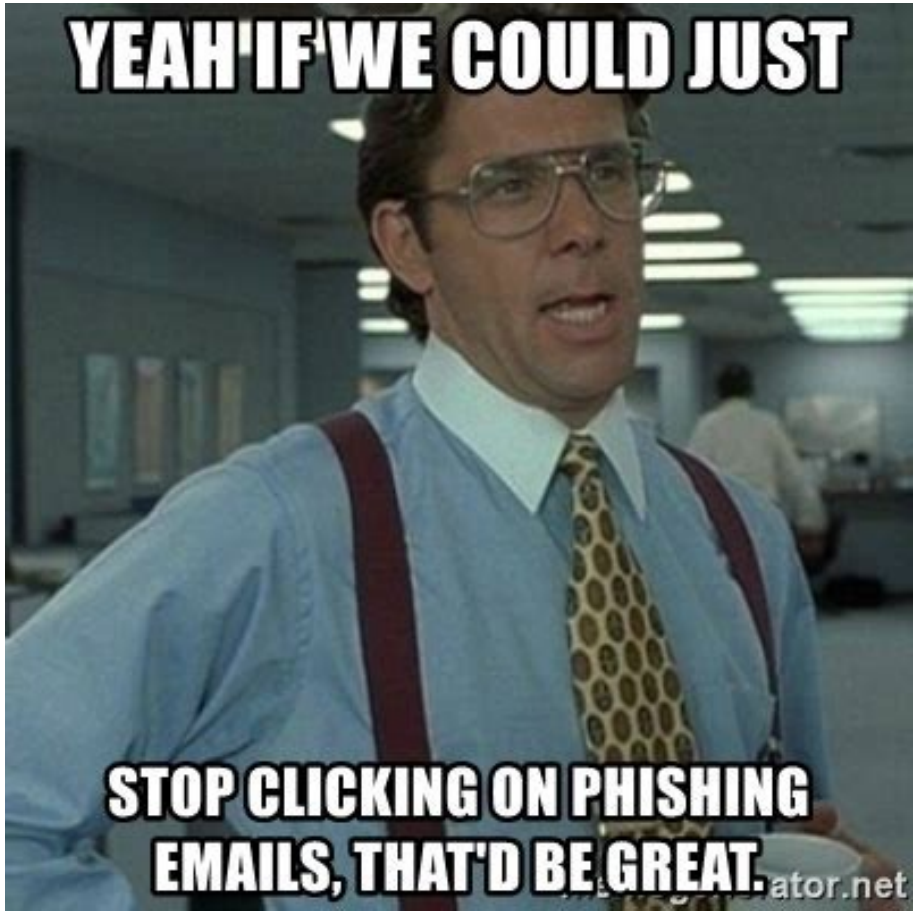
Juan Lavista Ferres
AI for Good Lab

This study investigates the effectiveness of multifactor authentication (MFA) in protecting commercial accounts from unauthorized access, with an additional focus on accounts with known credential leaks. We employ the benchmark-multiplier method, coupled with manual account review, to evaluate the security performance of various MFA methods in a largedataset of Microsoft Azure Active Directory users exhibiting suspicious activity. Our findings reveal that MFA implementation offers outstanding protection, with over 99.99% of MFA-enabled accounts remaining secure during the investigation period. Moreover, MFA reduces the risk of compromise by 99.22% across the entire population and by 98.56% in cases of leaked credentials. We further demonstrate that dedicated MFA applications, such as Microsoft Authenticator, outperform SMS-based authentication, though both methods provide significantly enhanced security compared to not using MFA. Based on these results, we strongly advocate for the default implementation of MFA in commercial accounts to increase security and mitigate unauthorized access risks.

33

https://go.microsoft.com/fwlink/?linkid=2238934&clcid=0x409&culture=en-us&country=us

Don’t Click the Link!



Chetrice Romero
April 24, 2024

Update Your Software

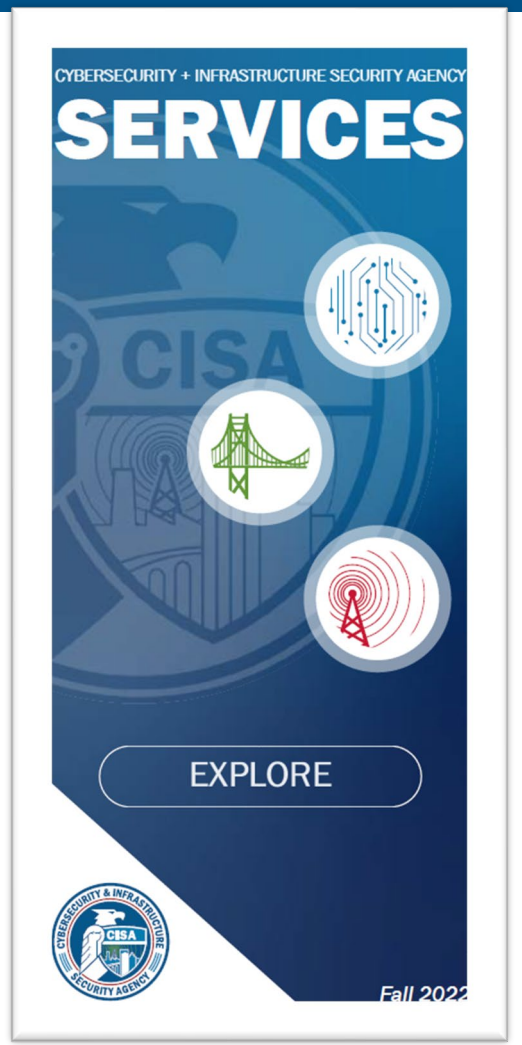
Chetrice Romero
April 24, 2024

Ask Your Vendors…

- ✓ What is your **password management program?**
- ✓ Do you require **multifactor authentication** wherever possible and is that an option for our product?
- ✓ Does your organization have cybersecurity training for all employees, especially around **phishing?**
- ✓ What is your **software and operating system patch program?** (CISA recommends regularly scanning internet-accessible hosts and remediating critical and high vulnerabilities within 15 and 30 days, respectively.)
- ✓ Do you have **cyber incident plan?**
- ✓ How and where is our data **backed up**?

Cybersecurity and Physical Services

- Cybersecurity Advisors
- Protective Security Advisors
- Cyber and Physical Assessments
- Vulnerability Scanning
- External Dependencies Management
- Tabletop Exercises (TTX)
- Training
- & more



Vulnerability Scanning by CISA

Known exploitable vulnerabilities are easy access for attackers, with **incidents averaging $100,000 in damages** for small and medium businesses.

CISA's free vulnerability scanning service helps **identify exposed assets and exploitable vulnerabilities** and is proven to reduce risk for participating organizations.

Avoid costly disruptions with early detection and action. Through weekly reports and timely alerts, we will help you **act before others take advantage.**

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

BY THE NUMBERS

- **7,200+** current customers nationwide
- **Over 3 Million** vulnerabilities found and fixed
- On average a **40% reduction in risk and exposure** by newly enrolled customers in their first 12 months
- Most enrollees see improvements within the first **90 days**

GETTING STARTED

Email vulnerability@cisa.dhs.gov
Subject: "Requesting Vulnerability Scanning Services"

Other CISA Services - Emergency Communications Coordination

- **Emergency Communications Coordination Program -** We employ subject matter experts located across the country to engage stakeholders and address the complex issues facing the emergency communications ecosystems
- **National Coordinating Center for Communications -** CISA's National Coordinating Center for Communications (NCC) continuously monitors national and international incidents and events that may impact emergency communications.
- **SAFECOM -** Through collaboration with emergency responders and elected officials across all levels of government, SAFECOM works to improve emergency response providers' inter-jurisdictional and interdisciplinary emergency communications interoperability across
- **Statewide Interoperability Plans and Planning Coordinators -** Statewide Communication Interoperability Plans (SCIPs) are locally-driven, multi-jurisdictional, and multi-disciplinary statewide plans to enhance emergency communications.

Other CISA Services – Chemical Security

- **ChemLock -** A completely voluntary program that provides facilities that possess dangerous chemicals no-cost services and tools to help them better understand their risks and improve their chemical security posture in a way that works for their business model.
- **Ammonium Nitrate Security Program (ANSP) -** The ANSP is a proposed regulatory program that seeks to reduce the likelihood of a terrorist attack involving the misuse of ammonium nitrate by creating a registration program for purchasers and sellers.

CHEM LOCK

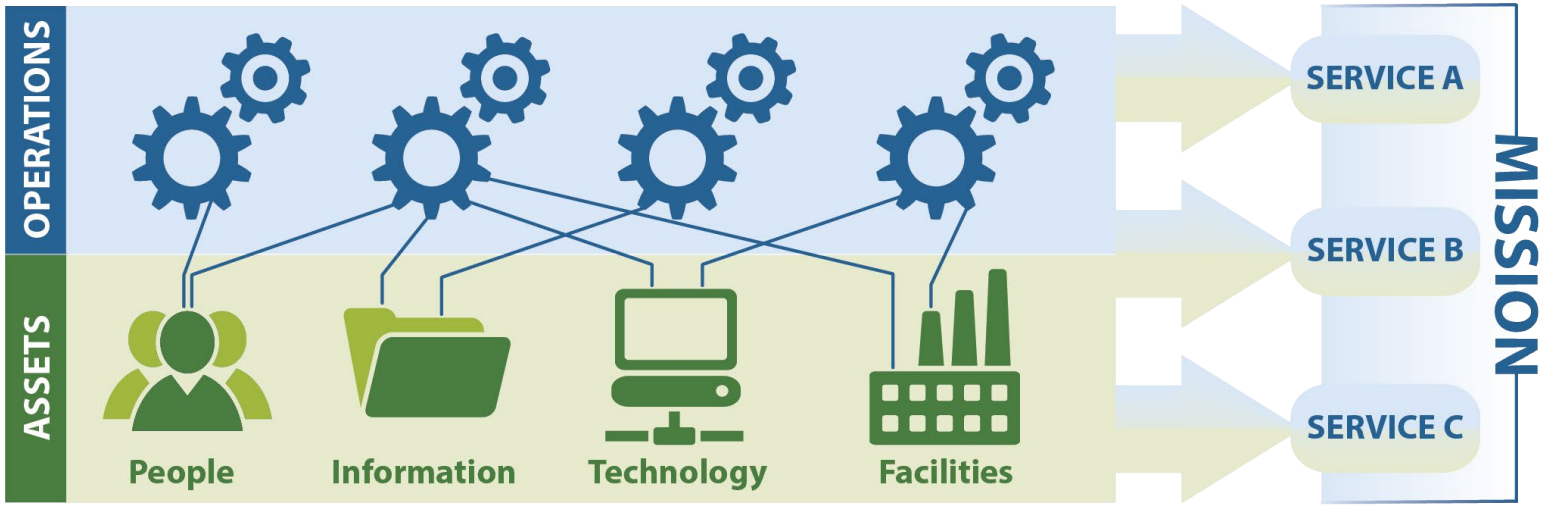
Know your chemicals.

Lock in your security posture.

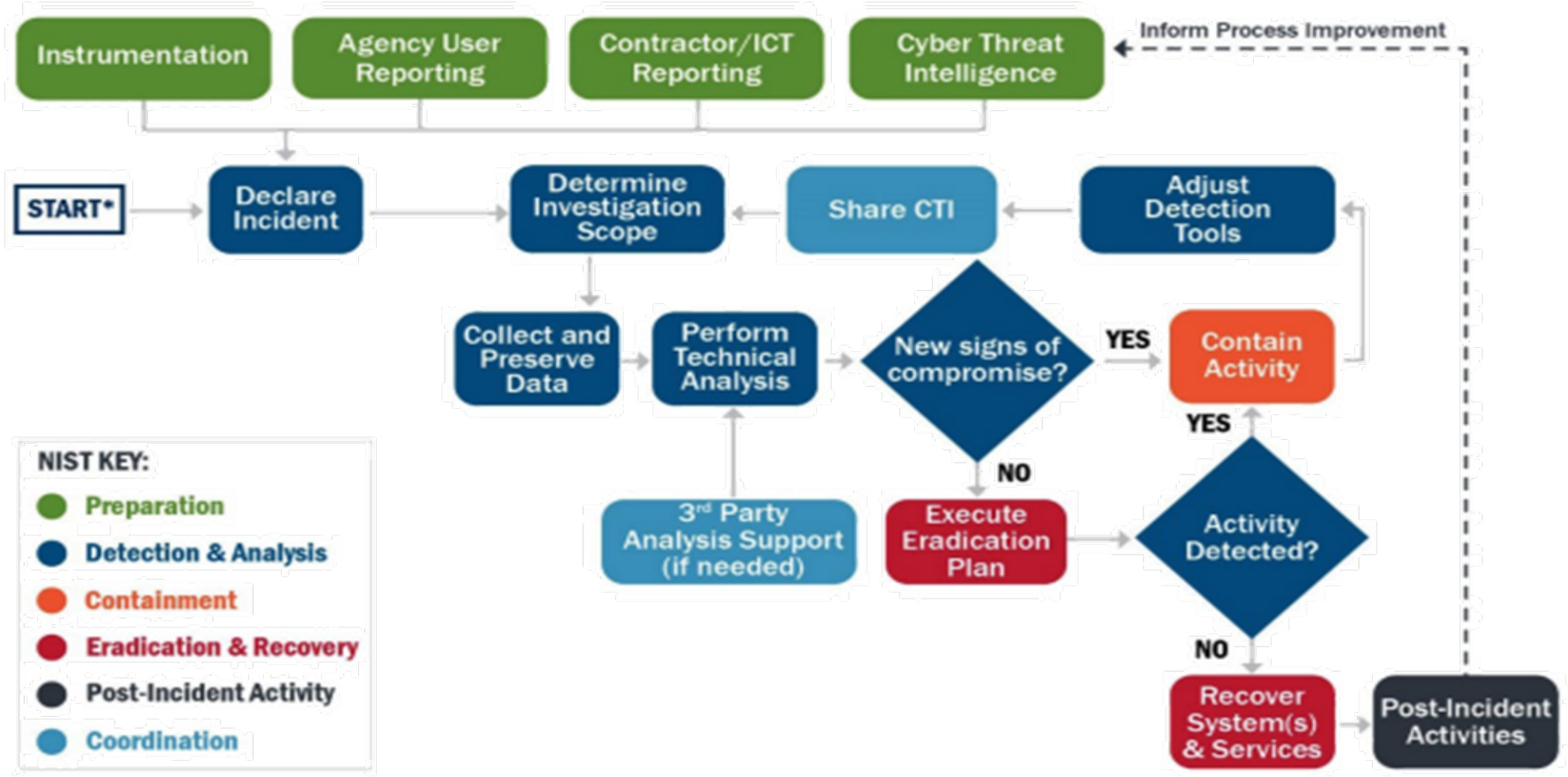
INCIDENT RESPONSE PLANNING, TRAINING, AND EXERCISING

Critical Services

- Identify your organization's critical service
  - Identify dependencies and interdependencies of these services
  - You can't protect what you don't know you have



Responding to a Cyber Attack



Incident Communications Process (cont.)

Establish a communications plan; ensure that it addresses methods and infrastructure.

Leverage any existing communications plan, infrastructure, and staff.

If no communications plan exists, create an incident communications plan with roles and responsibilities for each aspect of communication, including:

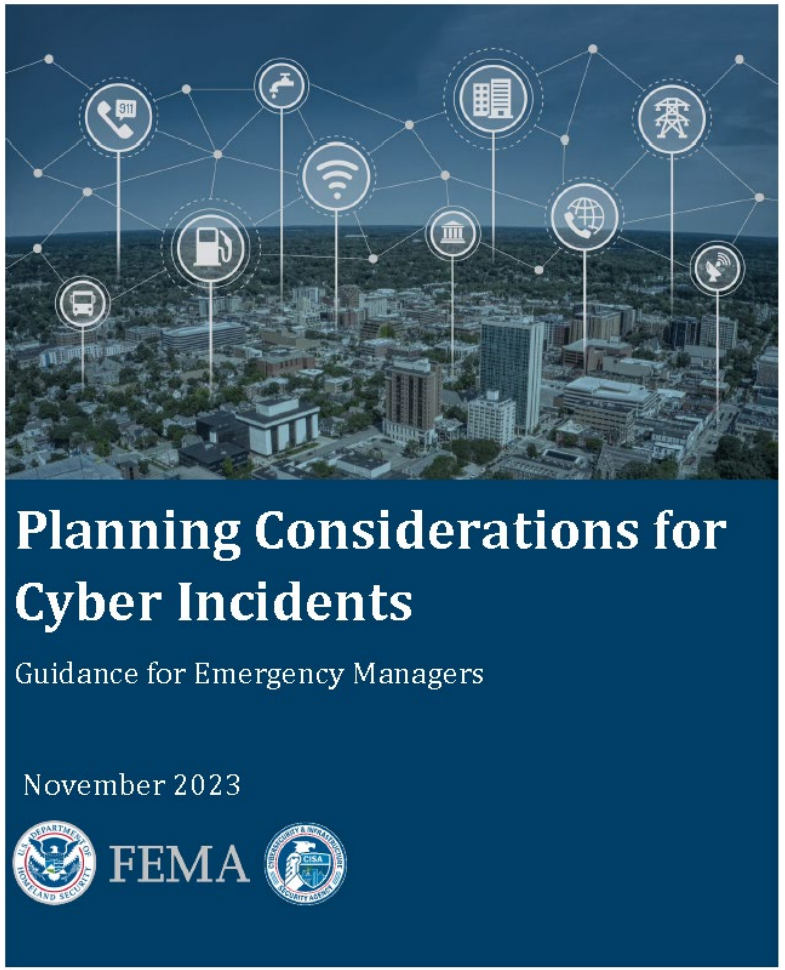
- External organization communication, including media
- Organization-wide communication
- Contact list initiation

Include Contacts In Your Plan

- Federal Resources
  - Cybersecurity & Infrastructure Security Agency (CISA)
    - CISA Central: 888-282-0807, central@cisa.gov
  - Federal Bureau of Investigation (FBI)
    - Cyber Watch: 855-292-3937, cywatch@fbi.gov
  - Additional agencies…
    - United States Secret Service (USSS)
    - Office of Intelligence and Analysis (I&A)
    - And many more….
- State Resources
- Regulators
- Key Partners in Community

FEMA/CISA Planning Considerations

- The guide provides state, local, tribal, and territorial emergency managers with foundational knowledge of cyber incidents to increase cyber preparedness efforts in their jurisdictions.
- This guide is intended to help emergency management personnel collaboratively prepare for a cyber incident and support the development of a cyber incident response plan or annex.
- Planning Guides | FEMA.gov



CISA Tabletop Exercise Packages

CISA Tabletop Exercise Packages (CTEPs) are a comprehensive set of resources designed to assist stakeholders in conducting their own exercises. Partners can use CTEPs to initiate discussions within their organizations about their ability to address a variety of threat scenarios.

With over 100 CTEPs available, stakeholders can easily find resources to meet their specific exercise needs.

https://www.cisa.gov/resources-tools/services/cisa-tabletop-exercise-packages

All CISA services and resources can be found by visiting www.CISA.gov

Contact Your Region
www.CISA.gov/about/regions

Chetrice Mosley-Romero
Indiana – CSA/CSC
Chetrice.Romero@cisa.dhs.gov

Additional Resources

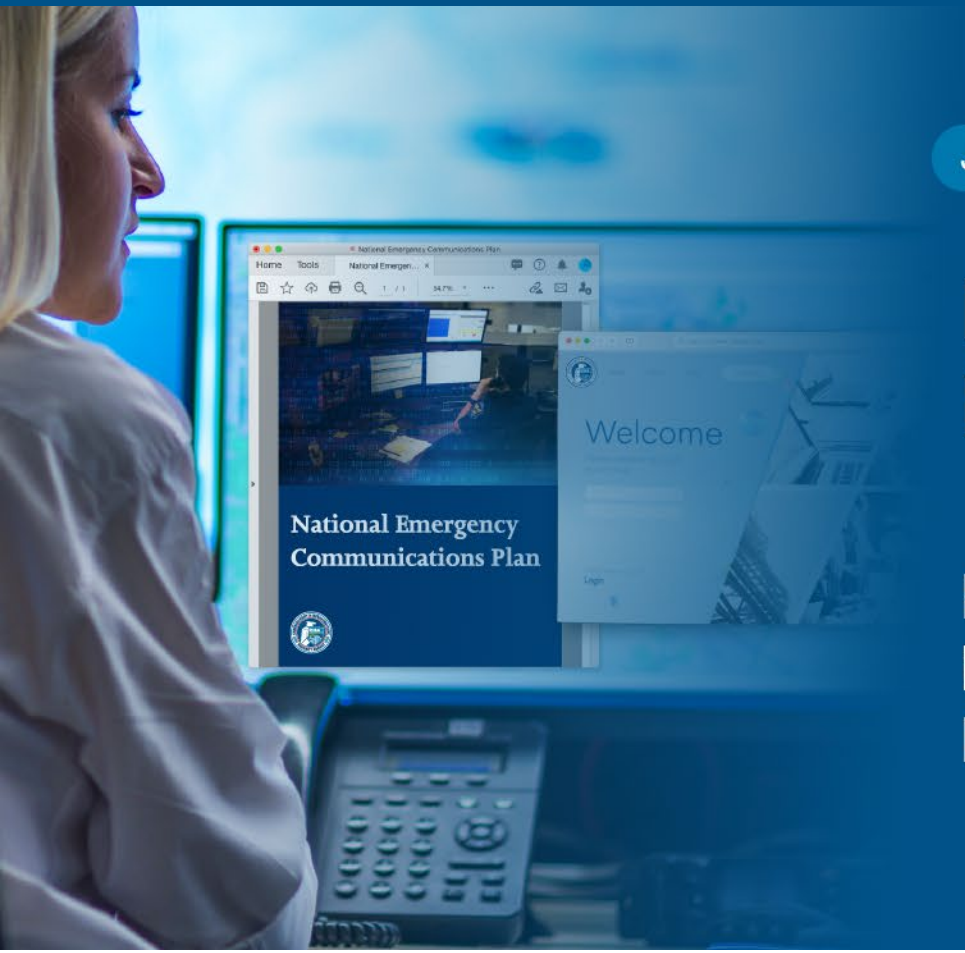
- National Emergency Communications Plan
- SAFECOM Nationwide Survey
- SAFECOM Interoperability Continuum
- Implementing Strong Authentication Capacity Enhancement Guide
- Implementing Number Matching in MFA Applications
- Implementing Phishing-Resistant MFA
- Next Level MFA: FIDO authentication
- How Fido Works

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 implement and maintain MFA
- **Collaborate** with subject matter experts to assist with cyber mitigation 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
SECURITY AGENCY
CISA