ESF-17 Cybersecurity

LDH Lunch and Learn

26 August 2021

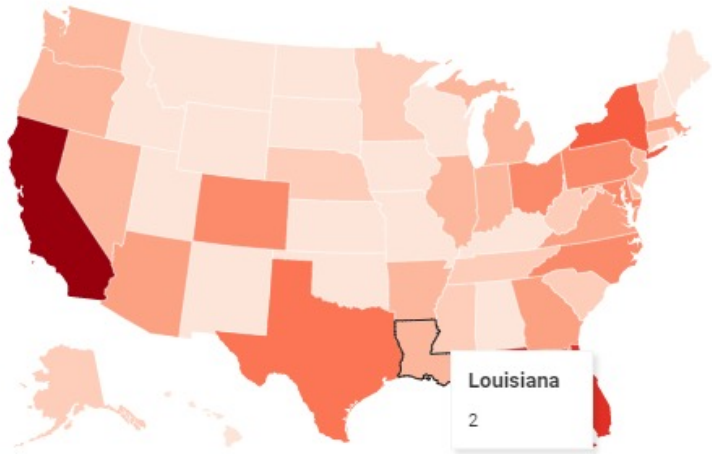
Senate Continuing Resolution 59 (SCR 59)

- Requests the Office of Public health of the Louisiana Department of Health to study and report relative to health care infrastructure needs in Louisiana

- Specifically notes the importance of a strong digital infrastructure

Recent Ransomware Attacks On Healthcare Organizations

- In 2020, 92 individual ransomware attacks affected over 600 separate clinics, hospitals, and organizations and more than 18 million patient records
- 60 percent increase from 2019
- Estimated cost of these attacks is almost $21 billion
- Downtime varied from minimal impact due to frequent data backups to weeks or months of paper only systems



Louisiana Cyber Attacks 2021 YTD

- 24 Total Cases involving critical infrastructure:
  - 4 – Chemical Cases
  - 1 - Commercial Facilities
  - 3 - Emergency Services
  - 2 - Financial Services
  - 1 - Healthcare and Public Work
  - 5 - Information Tech
  - 1 – Transportation
  - 7 – Governmental Facilities
- Estimated $600 Million Financial Loss Year to Date

Why Are Hospitals Targeted

- They are considered easy targets
- Critical Nature of Healthcare Makes It More Likely Hospitals Will Pay Ransom
- Lack Of Training
- Remote Work Is Often Necessary In Healthcare
- Unsecure Medical Devices/Outdated Technology
- Vulnerable to Supply Chain Attacks
- https://www.youtube.com/watch?v=jvy1km54Rpg

Who Conducts Cyber Attacks?

- Cyber-Criminals
- Cyber Terrorists
- Nation States
- Hackers
- Hacktivists
- Insider Threat

Cyber Threats

Phishing - Attacker attempts to steal sensitive or personally identifiable information by pretending to be a trustworthy source

Malware – software that is designed to damage a computer, server, client, or network

- Ransomware – attacker blocks access to user's data and demands compensation to restore access or prevent public release
- Viruses – malicious code that replicates and spreads itself throughout a network
- Trojans – malicious code that is disguised as legitimate software

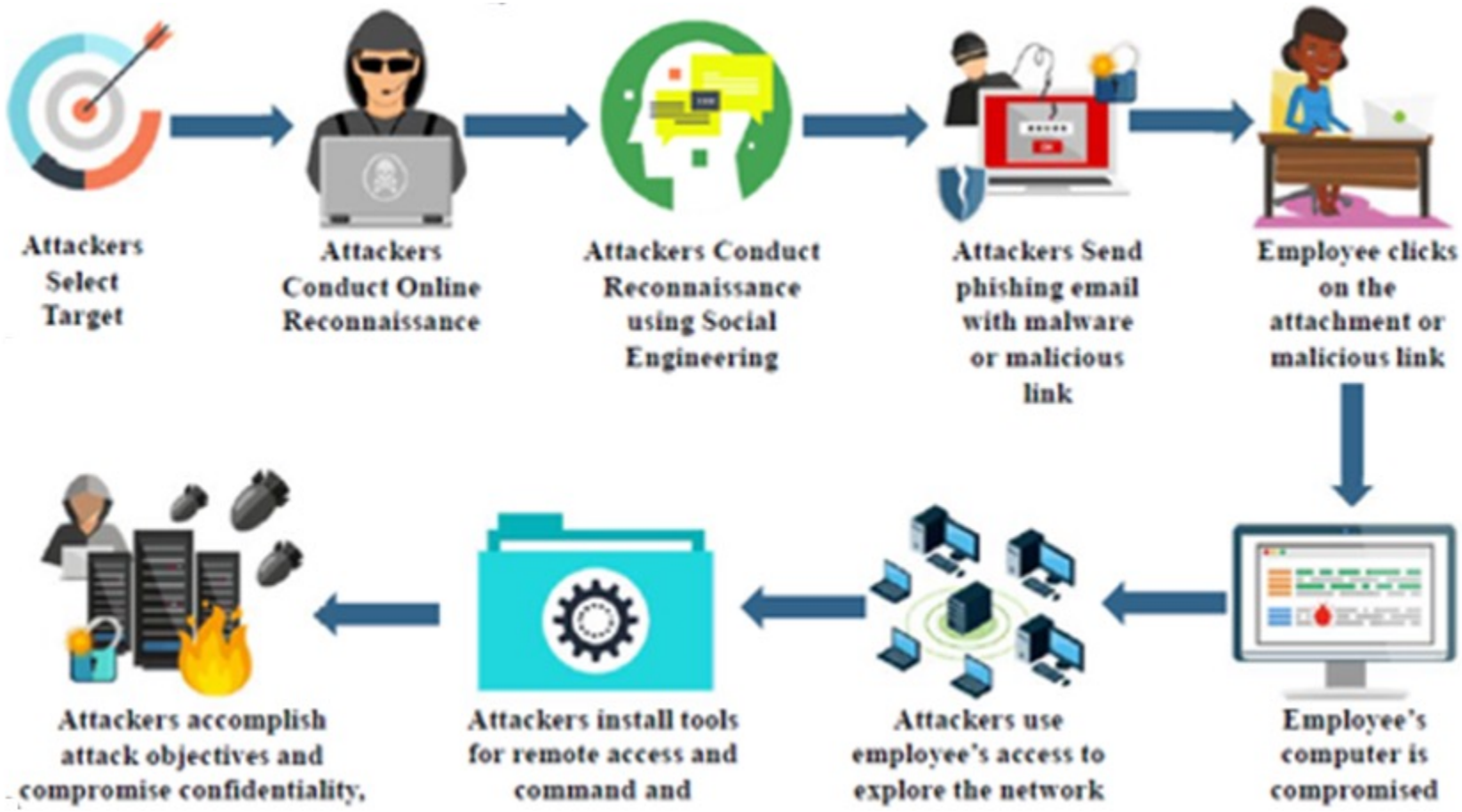
Denial-of-service (DoS) or distributed denial-of-service (DDoS) attack - Flood networks, servers, and or systems with traffic, rendering them inaccessible for users

Man-in-the-middle attack – attacker intercepts communication between two users or systems and steals or alters the data

Software Security Vulnerabilities – attackers exploit vulnerabilities in operating systems and software to gain access to networks, elevate privileges, and/or introduce malware into a network

Supply Chain Attacks - an adversary slips malicious code or even a malicious component into a trusted piece of software or hardware

How Do Cyber Attacks Occur



https://www.youtube.com/watch?v=C47wzCejotc

How To ~~Prevent~~ Minimize Likelihood Of Cyberattacks

- Keep all software installed on your Computers and Servers updated & patched while also using End Point Protection Software
- Use Multi-Factor Authentication whenever possible for Professional or Financial internet services
- Use VPN with Multi-Factor Authentication when remotely accessing your network
- Don't allow users to browse the internet and read email while logged on as an admin user, least privilege principles are recommended
- Ensure network firewall and intrusion prevention logs are monitored for signs of compromise
- Maintain at a minimum weekly backups that are stored offsite and offline
- Make yourself an unattractive target
- Segmentation between Operational Technology(OT)/Industrial Control System(ICS) networks and Information Technology(IT) networks

Vulnerability Assessments/Risk Analysis

- Vulnerability Assessments are a recommended to identify vulnerabilities in your network and facilitate Risk Analysis and Threat Mitigation.
- NCCIC ICS Cyber Security Evaluation Tool (cisa.gov)
  - The Cyber Security Evaluation Tool (CSET®) provides a systematic, disciplined, and repeatable approach for evaluating an organization's security posture.
  - CSET Detailed Tutorial – YouTube

Managed Service Providers

Cybersecurity Services are a necessary and important component of Managed IT Contracts. Consider addressing the following in any such contracts:

- 24/7 Monitoring
- Access Control
- Data Security
  - Backup
  - Encryption
- Security Updates
- Domain Security
- Email Security
  - Anti-Spam & Anti-Malware
  - Phishing Isolation
- End-Point Security
  - Anti-Malware Protection
  - Content Filtering
- Network Security
- Cloud Security
- Security Training For Staff
- Risk Assessment and Gap Analysis
- Incident Response

How To Prepare For Response

- **Have a Cyber Incident Response Plan/COOP** - Identify all critical data and systems. Ensure regular backups of these systems and data are conducted. Develop a continuity of operations plan (COOP) so that services can be quickly restored in the event of a Cyber Attack.
- **Conduct Exercises** – Plan and conduct exercises which execute cyber incident response ,COOP, and communication plans in order to identify gaps in plans and ensure staff are prepared to respond.
- **Improve Plans** – Use lessons learned to eliminate gaps in plans.
- Cybersecurity Framework | NIST

What To Do If You Are A Victim Of A Cyber Attack

- If you believe you have already become a victim of a cyber-attack, the following steps are vital to minimizing service interruption and ensuring the proper evidence collection process is followed:
- DO NOT Power Off Servers or Workstation, as this causes more harm than good.
- DO Notify IT/Security Personnel
- DO Physically Disconnect the Network connections, (or firewall) to prevent outbound traffic.
- DO Disable remote access or VPN
- DO Install Any Pending Security Updates or Patches
- Contact Louisiana State Police Fusion Center: 1-800-434-8007 LaFusion.Center@la.gov

ESF-17 Cybersecurity Overview

Purpose

- The State of **Louisiana** Emergency Operations Plan (EOP) identifies State Emergency Support Functions **(ESFs**) as the structure for organizing and coordinating State resources by area of function.
- ESF 17 – Cyber Incident Response.
- Key State Agencies – GOHSEP\STATE POLICE\LANG\OTS

Scope

- State services under this ESF consists of the **identification**, **mobilization** and **coordination** of available state owned, private industry and volunteer personnel and equipment essential to **respond**, **investigate**, **contain**, **recover**, and otherwise **manage**:
    1. Any significant Cyber incident impacting state entities
    2. Cyber disruptions of critical infrastructure; before, during and after an impending, suspected, or actual incident.

State Assistance Capabilities

- Louisiana State Analytical & Fusion Exchange (LA-SAFE)
  - Receive, analyze, and alert on the threat events from federal or private orgs.
  - Serve as primary liaison to all local, state, and federal law enforcement agencies
  - Coordinate CIRT resources for evidence collection
- Louisiana National Guard (LANG)
  - Co-lead cyber incident response efforts
  - Provide Defense Cyber Operations Element (DCOE) and Cyber Protection Team (CPT) to assist with cyber incident response
- Division of Administration (DOA)/Office of Technology Services (OTS)
  - Co-lead cyber incident response efforts
  - Provide Chief Information Security Officer (CISO) and Information Security Teams (IST) to assist with cyber incident response
- Governor's Office of Homeland Security and Emergency Preparedness (GOHSEP)
  - Serve as Incident Response Coordinator
  - Coordinate with local officials for resource requests, reporting, and communication throughout cyber incident response

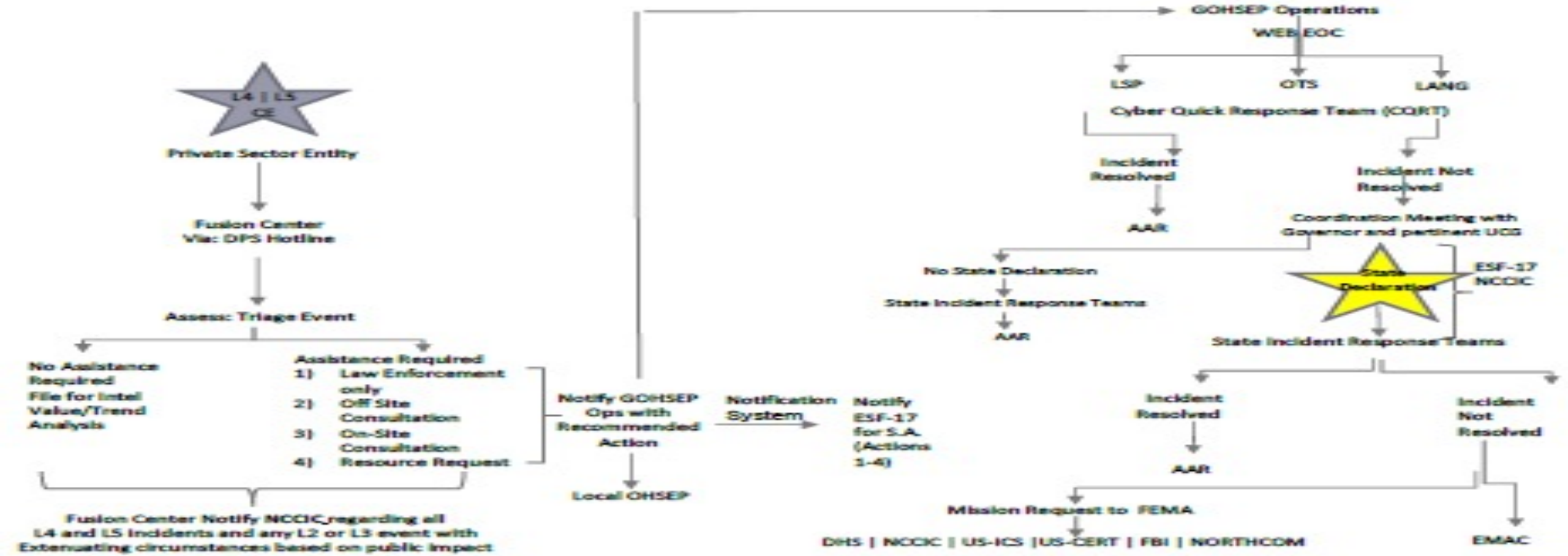
ATTACHMENT 4

CYBER INCIDENT RESPONSE MANAGEMENT SUPPORT TO A PRIVATE SECTOR ENTITY

Cyber Event

L5 (EMERGENCY) – Poses an imminent threat to the provision of wide-scale CI services, state gov't stability, or the lives of LA citizens
L4 (SEVERE) – Likely to result in a significant impact to public health or safety

Cyber Response Assets	Cyber Acronyms
LANG: INCIDENT RESPONSE TEAMS	NCCIC: NATIONAL CYBERSECURITY & COMMUNICATIONS INTEGRATION CENTER
DOA-OTS: INCIDENT RESPONSE TEAMS	MS-ISAC: MULTI STATE CENTER FOR INTERNET SECURITY
LSP: EVIDENCE TEAM/CRITICAL INFRASTRUCTURE	USCERT: UNITED STATES COMPUTER EMERGENCY READINESS TEAM



Additional Resources

- Louisiana Get a Gameplan https://getagameplan.org/make-a-plan/cybersecurity-plan/
- Cybersecurity & Infrastructure Security Agency https://www.cisa.gov/cybersecurity
- National Institute of Standards and Technology https://www.nist.gov/cyberframework

Senate Continuing Resolution 59 (SCR 59)

- Include Cybersecurity/IT Infrastructure Gaps

- Vulnerability assessments can help identify gaps in your cyber infrastructure

QUESTIONS

GOHSEP POCs:
(Asst. Dpty. Director Homeland Security) Neal Fudge 225-721-1808 Neal.Fudge@la.gov
(Cyber Security Prog. Mgr.) Matthew McKey 225-266-7732 Matthew.J.McKey@la.gov