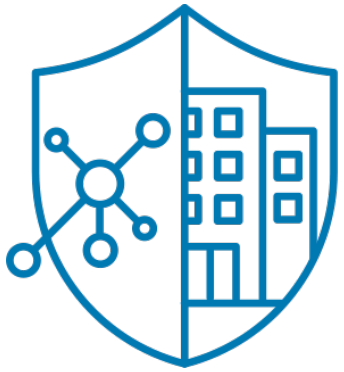
INCIDENT RESPONSE WEBINAR SERIES #9

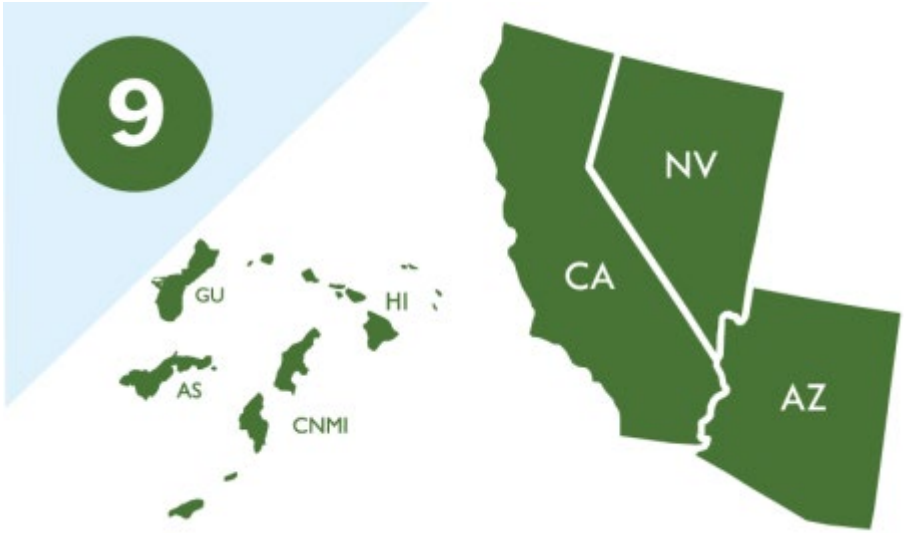
Jennilyn Labrunda
Cybersecurity Advisor (Guam, CNMI, & AS)
CISA, Region 9

About CISA

Mission: Lead the national effort to understand, manage, and reduce risk to our nation's cyber and physical infrastructure.

Vision: A secure and resilient critical infrastructure for the American people.



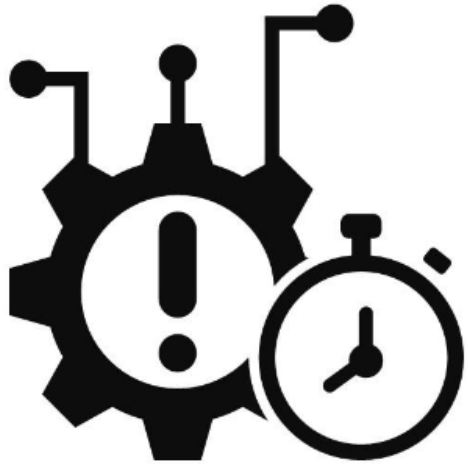


Agenda

- Importance of Incident Response Plan
- Understanding Cybersecurity Incidents
- Phases of Incident Response
- Q & A

Why Incident Handling Matters

- Minimize damage
- Maintain customer trust
- Regulatory compliance
- Financial implications of breaches



Sector-Specific Impacts

- Healthcare: Patient data breaches
- Finance: Financial fraud
- Water/Wastewater: Critical infrastructure attacks
- IT: Intellectual property theft
- Local Government: Ransomware attacks

What is a Cybersecurity Incident?

- Event that jeopardizes the C-I-A of your information systems

HIGH **Handle Immediately** **(Impact Cost: > $100,000)** **Cyber Crisis** **Serious/significant impact**	
MEDIUM **Handle within 1-4 hours** **(Impact Cost: > $25,000 but < $100,000)**	**LOW** **Handle within 3 Days** **(Impact Cost: < $25,000)**
Moderate Impact	**No impact to sensitive data** **Impact noncritical systems**

Incident: Confidentiality Compromise

- **Unauthorized Access:** any access for which permission has not been granted.
  - Unauthorized permissions to connect, authenticate, read, write, create, delete, modify, etc.
  - Can be logical or physical
  - Can be by an individual or another system
  - Ex: Malware infection, stolen equipment, data breach

- **Inappropriate Usage:** acceptable use policies are violated which may include what types of data may be accessed or transmitted, how information may be accessed or transmitted, and where information may be received from or transmitted to.
  - Ex: E-mail compromise, misuse of privileges

Incident: Integrity compromise

- An incident by which data has been erroneously modified to achieve fraudulent activities, damage the company's reputation, and/or influence public opinion and behavior
  - Man-in-the-middle attacks
  - Data tampering
  - SQL injections
  - Ransomware

Incident: Availability compromise

- Authorized users are unable to access and use information systems, data, and resources when needed.
  - System downtime
  - Data inaccessibility
  - Delayed response
  - Service interruptions

Ex: Ransomware, DDoS, data corruption, physical security breach, power or internet outage

Incident Severity Level: HIGH

HIGH
Handle Immediately
(Impact Cost : > $100,000)

Cyber Crisis: Disruptions that are serious/ Likely to result in significant impact to services and/or large volumes of sensitive data exposure

INCIDENTS CLASSIFIED AS HIGH		
A breach of certain types of data, including FTI, PII, HIPAA data, or data implicating PCI-DSS, that pose a significant risk to personal privacy or a significant risk of individual financial loss	Malware posing a significant wide-ranging risk to system operations or a significant risk of a large-scale data breach	Computer virus/worms/Trojans for which anti-virus software updates are not available
Suspected computer or network break-in	Website defacements or compromises	Successful denial-of-service (DoS) attacks
Serious violations of acceptable use policies	Any violation of law	

Incident Severity Level: MEDIUM

MEDIUM
Handled within 1-4 hours, but certainly Same Day (Impact Cost Less than $100,000 – more than $25,000)
Potentially Serious Likely to result in impact to services and/or some data exposure

INCIDENTS CLASSIFIED AS MEDIUM		
Intrusion Detection System reports that define activity as medium	Property destruction related to a security incident (less than $100,000)	Personal theft related to a security incident (less than $100,000)
Misuse of organizational property, facilities, and services	Unconfirmed computer virus/ worms (depending on operational impact)	Employee clicked on a phishing link

Incident Severity Level: LOW

LOW Handle within 3 Days (Impact Cost: < $25,000)
Least Severe might impact 5 or less systems No impact to sensitive data Impact noncritical systems

INCIDENTS CLASSIFIED AS LOW		
Minor misuse of organization property, facilities, and services	Detected virus/worms with minimal operational impact	Employee Installed unsupported unharmful software

Incident Triage

- Identify the incident compromise: C-I-A
- Categorize the severity of the incident
- Ex: Malware affecting financial accounting system

	Confidentiality	Integrity	Availability
Low			
Medium			X
High	X		

Case Study: Ransomware in Action

- **Royal Mail Ransomware Attack (January 2023)**
- **Incident Overview**:
  - In January 2023, Royal Mail was hit by a ransomware attack from the LockBit group.
  - The attack disrupted international shipping services by encrypting crucial operational data.
- **How It Occurred**:
  - Attack began with a phishing email.
  - The attackers gained access to Royal Mail's systems and encrypted files, demanding a ransom for decryption.

Case Study: Ransomware in Action

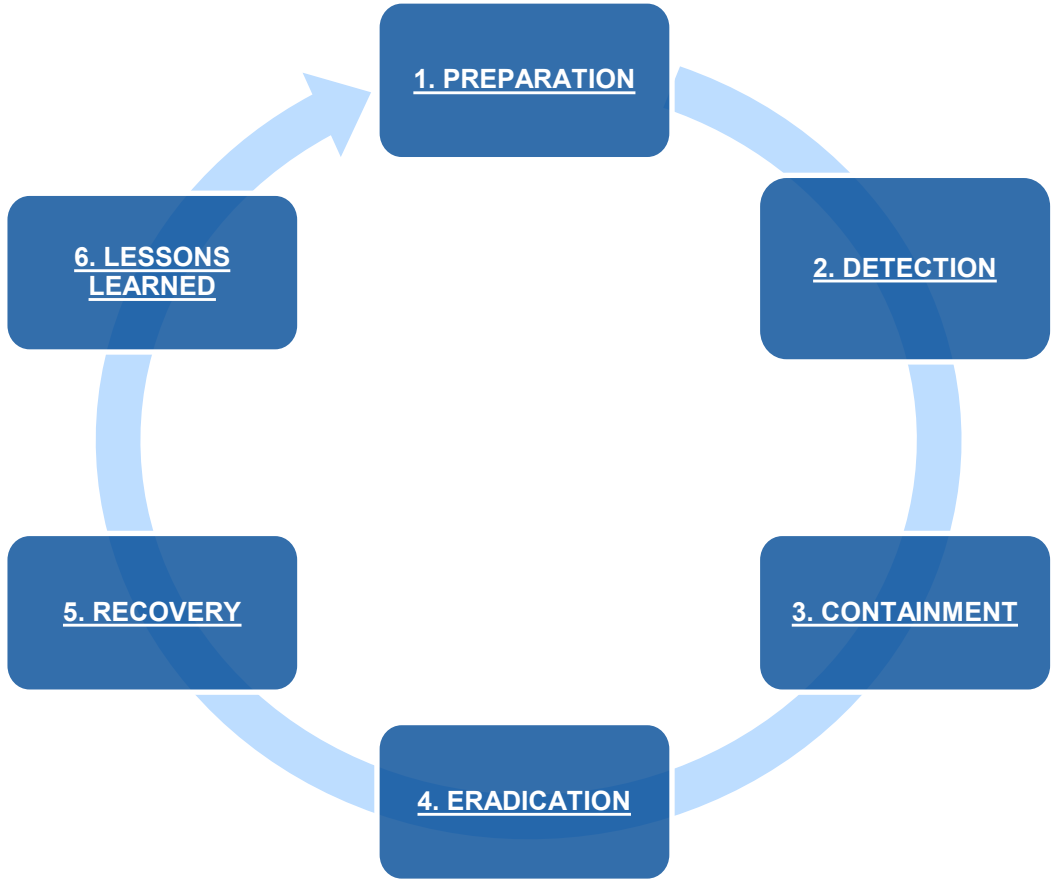
- **Consequences**:
  - Operational Disruption: International deliveries were suspended.
  - Reputational Damage: Royal Mail's image during a period of heightened cyber risk.
  - Financial Losses: Operational halts, recovery costs, and ransom payments led to financial impact.
  - Customer Impact: Delayed shipments caused frustration and loss of trust.
- **Lessons Learned**:
  - Strengthen Email Security: Train staff on phishing and implement better email filtering.
  - Backups & Recovery: Ensure regular backups and business continuity plans.
  - Detection Tools: Deploy advanced ransomware detection and prevention tools.
  - Incident Response: Maintain a robust, tested incident response plan.

Quick Poll: Your Biggest Concern

- Options: Data breach, ransomware, phishing, insider threats

Phases of Incident Response

- Preparation
- Detection and Analysis
- Containment, Eradication, and Recovery
- Post-Incident Activity



Example Incident Response process based off NIST SP 800-61r2

Phase 1: Preparation

- Develop policies and procedures
  - Establish an incident response team: internal and external
  - Employee training
  - Tools and resources readiness

Phase 1: Preparation – IRT (Security/IT)

Roles	Responsibilities
Chief Information Security Officer (CISO), CIO, CTO or equivalent	• Incident Response Team (IRT) Lead and overall response to security incident (form team, assign task to appropriate skillsets, review containment plan and eradication), assess threat level, involve outside law enforcement and other agencies as needed. • Liaison with upper management, other teams and organizations as well as brief executive leadership • Work with Risk Management to coordinate reporting to Insurance carrier • Defuse Crisis situation • Ensure appropriate IT resources (staff and equipment) are allocated to assist with handling the incident
Information Security Analyst, Cybersecurity Analyst,	• Coordinate the IRT Activities • Gather Information • Log details of the incident • Provide incident updates to CISO and to other necessary groups • Analyze Malware to determine its purpose or intent • Use Forensics tool to investigate what transpired • Detect network and system intrusion
IT Operations Team (SysAdmin, NetAdmin, DB Admin, Web Dev)	• Assist with intrusion detection, investigation, and remediation
Desktop Support, Service Desk, Helpdesk	• Carry out scripted tasks provided by IRT • Triage computers infected with malware • Run antivirus scans • When necessary, retrieve and reimage machines

Phase 1: Preparation – IRT (Management)

Roles	Responsibilities
CEO/Executive Leader	• Communicate security incident to Council or board members • Determine whether Emergency operation center should be activated • If applicable, determine if open to negotiation with cyber criminals
Attorney	• Provide legal advice as requested • Involved in all matters involving Personal Information or security incidents involving Medium or higher severity levels • Review impact of incidents to ensure the company meets specific requirements for state and exposure types • Review correspondence relating to PII and security breaches • Assist when it is believed that the incident may have legal ramifications, including evidence collection prosecution of suspect lawsuits
Finance	• Assist with allocation of additional funding needed to contain and remediate incident activities. • Assist with payroll, credit card and other financial activities.
Human Resources	• Assist in the drafting of internal communications to employees when necessary. • Assist with disciplinary proceedings for any employee(s) suspected of causing an incident (i.e. email harassment, sabotaging systems, injecting malware on systems or other malicious activity).
Public Information Officer	• Oversee all communications involving personal information and security incidents identified by the team. • Coordinate activities of the communication unit. • Handle media communications.

Phase 1: Preparation – IRT (External)

Agency	Potential Areas of Assistance
CISA (Cybersecurity and Infrastructure Security Agency) IRF Incident Reporting Start - IRF (cisa.gov) https://www.cisa.gov/report	• Analyzes the potential impact across critical infrastructure, investigates those responsible in conjunction with law enforcement partners, and coordinates the national response to significant cyber incidents • SME to provide guidance and recommendations to improve security • Malware Analysis | CISA • IRT tabletop exercise
FBI Internet Crime Complaint Center(IC3) | File a Complaint https://www.ic3.gov/	• Assist in forensic investigation, and prosecution (as applicable) of cybercriminal • FBI deploys personnel to conduct an investigation, slighty different from incident response. • Potentially provide specific advice on mitigating particular vulnerabilities or intrusion vectors. • May share information during course of investigation, could assist victim with remediation
Software/Hardware Vendor	• Assist with identifying/determining suspicious activity, gathering logs, determining false positive activity, software/hardware vulnerability threats known by the vendor
Internet Service Provider	• Assist with investigation and remediation activities related to ISP services • Assist with in blocking a major network-based attack or tracing its origin
External/Vendor Incident Response Team	• Rapid response; quickly deploy experts to assess the situation • Determine scope and severity of incident • Help isolate affected system and implement immediate mitigation measures • Offer round-the-clock assistance and provide a dedicate team focused solely on resolving crisis

Phase 1: Preparation – Contacts Worksheet

- Incident Response Team and Key Contacts Worksheet

Incident Response Team and Key Contact Information Worksheets

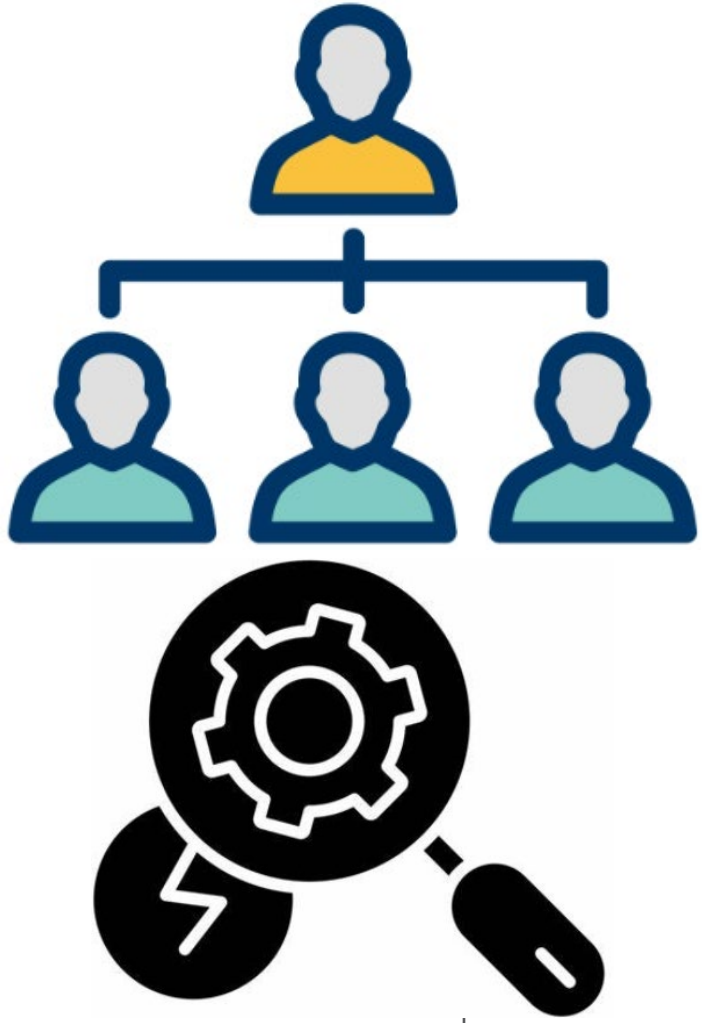
The following worksheet was derived from Cybersecurity and Infrastructure Security Agency (CISA) *Cyber Incident Detection and Notification Planning Guide for Election Security*.

INTERNAL Information Technology and Management Leads

Role	Name	Contact Information (Phone and Email)
CISO	**Primary:** [Insert Primary Name and Affiliation] **Backup:** [Insert Backup Name and Affiliation]	**Primary:** [Insert Primary Phone and Email] **Backup:** [Insert Backup Phone and Email]
CIO or CTO	**Primary:** [Insert Primary Name and Affiliation] **Backup:** [Insert Backup Name and Affiliation]	**Primary:** [Insert Primary Phone and Email] **Backup:** [Insert Backup Phone and Email]
Cybersecurity Analyst or Information Security Analyst	**Primary:** [Insert Primary Name and Affiliation] **Backup:** [Insert Backup Name and Affiliation]	**Primary:** [Insert Primary Phone and Email] **Backup:** [Insert Backup Phone and Email]
Network Admin	**Primary:** [Insert Primary Name and Affiliation] **Backup:** [Insert Backup Name and Affiliation]	**Primary:** [Insert Primary Phone and Email] **Backup:** [Insert Backup Phone and Email]
System Admin	**Primary:** [Insert Primary Name and Affiliation] **Backup:** [Insert Backup Name and Affiliation]	**Primary:** [Insert Primary Phone and Email] **Backup:** [Insert Backup Phone and Email]
Server Admin	**Primary:** [Insert Primary Name and Affiliation] **Backup:** [Insert Backup Name and Affiliation]	**Primary:** [Insert Primary Phone and Email] **Backup:** [Insert Backup Phone and Email]
Database Admin	**Primary:** [Insert Primary Name and Affiliation] **Backup:** [Insert Backup Name and Affiliation]	**Primary:** [Insert Primary Phone and Email] **Backup:** [Insert Backup Phone and Email]
Operational Technology Admin	**Primary:** [Insert Primary Name and Affiliation] **Backup:** [Insert Backup Name and Affiliation]	**Primary:** [Insert Primary Phone and Email] **Backup:** [Insert Backup Phone and Email]
Helpdesk	**Primary:** [Insert Primary Name and Affiliation]	**Primary:** [Insert Primary Phone and Email] **Backup:** [Insert Backup Phone and Email]

Building a Communications Plan

- Identify the key members of the incident response communications team
- Develop your “common terms” list.
- Establish your internal staff communications plan and external communications approval process
- Identify and test your communications assets
- Develop a template for communicating during an incident response



Quick Poll: Incident Response Team

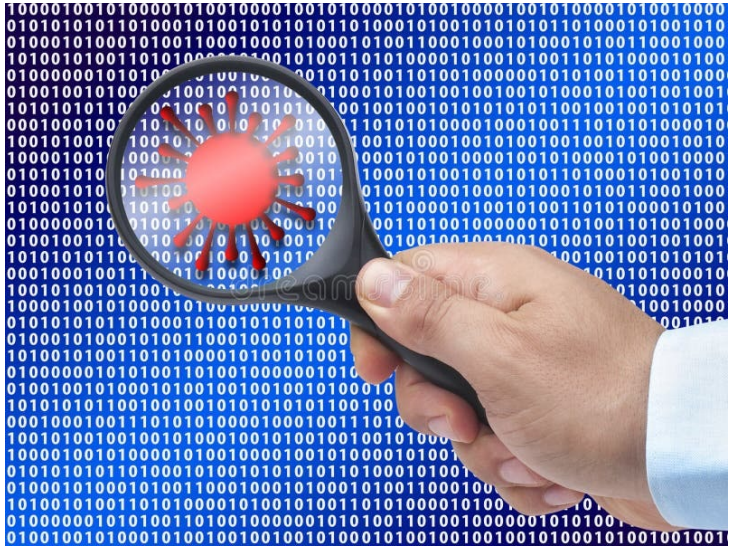
- Who would you consider adding to an incident response team?

Resources for Incident Response Plans

- Federal Government Cybersecurity Incident and Vulnerability Response Playbooks
  - https://www.cisa.gov/sites/default/files/publications/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf
- Water and Wastewater Sector - Incident Response Guide | CISA
  - https://www.cisa.gov/resources-tools/resources/water-and-wastewater-sector-incident-response-guide
- Election Infrastructure Incident Response Communications Guide | CISA
  - https://www.cisa.gov/resources-tools/resources/election-infrastructure-incident-response-communications-guide
- Public Power Cyber Incident Response Playbook
  - https://www.publicpower.org/system/files/documents/Public-Power-Cyber-Incident-Response-Playbook.pdf
- #StopRansomware Guide | CISA
  - https://www.cisa.gov/stopransomware/ransomware-guide
- SP 800-61 Rev. 2, Computer Security Incident Handling Guide | CSRC (nist.gov)
  - https://csrc.nist.gov/pubs/sp/800/61/r2/final
- Information Security Policy Templates | SANS Institute
  - https://www.sans.org/information-security-policy/

Phase 2: Detection and Analysis

- Detection and Monitoring systems
  - Anti-virus, Endpoint Detection & Response (EDR), Intrusion Detection/Prevention Systems (IDS/IPS), Data Loss Prevention, Security Information and Event Management (SIEM)
- Incident indicators
- Initial assessment
- Prioritization of incidents



Communications During an Incident

- Gather the Facts
- Activate Your Response Communications Process
- Notify Key Internal Stakeholders and Partners
- Communicate to Key External Stakeholder
- Consider issuing an initial public statement
- Maintain Continous Public Communications Updates
- Gather External Feedback and Adjust Communication Delivery

Phase 3: Containment

- **Containment** - immediate actions to contain threats
  - Isolate infected Systems
    - Disconnecting compromised machines
    - Implementing network segmentation
  - Block Malicious IPs
    - Update firewall rules
    - Implement stricter access controls
  - Disable compromised user accounts
    - Force password resets

Phase 4: Eradication

- **Eradication** - removing the cause of the incident
  - Remove malware
  - Patch vulnerabilities
    - Apply security updates to all systems
    - Close any exploit paths identified during the incident
  - Clean or reimage systems
    - Restore from clean backups where possible

Phase 5-6: Recovery and Post-Incident

- **Recovery** - restoring systems and data
  - Bring cleaned system back online gradually
  - Monitor for abnormalities
    - Implement enhanced logging and monitoring
  - Implement security improvements
- **Post-incident** – documenting lessons learned
  - Review of response procedures
  - Impact assessment
  - Update IRP
  - Educate employees about the incident and prevention measures

Scenario Exercise

- Imagine your organization discovers that a critical system has been compromised by malware. What would you do first?
  A. Shut down the system immediately
  B. Notify your IT team
  C. Contact law enforcement
  D. Ignore it and hope for the best

For more information:
www.cisa.gov

Questions?

Jennilyn Labrunda
Cybersecurity Advisor (Guam, CNMI, & AS)
CISA, Region 9
jennilyn.labrunda@cisa.dhs.gov
M: **808-260-3143**


CYBERSECURITY & INFRASTRUCTURE
CISA
SECURITY AGENCY