Cyber Incident Management and Response Plan (REVIEW)

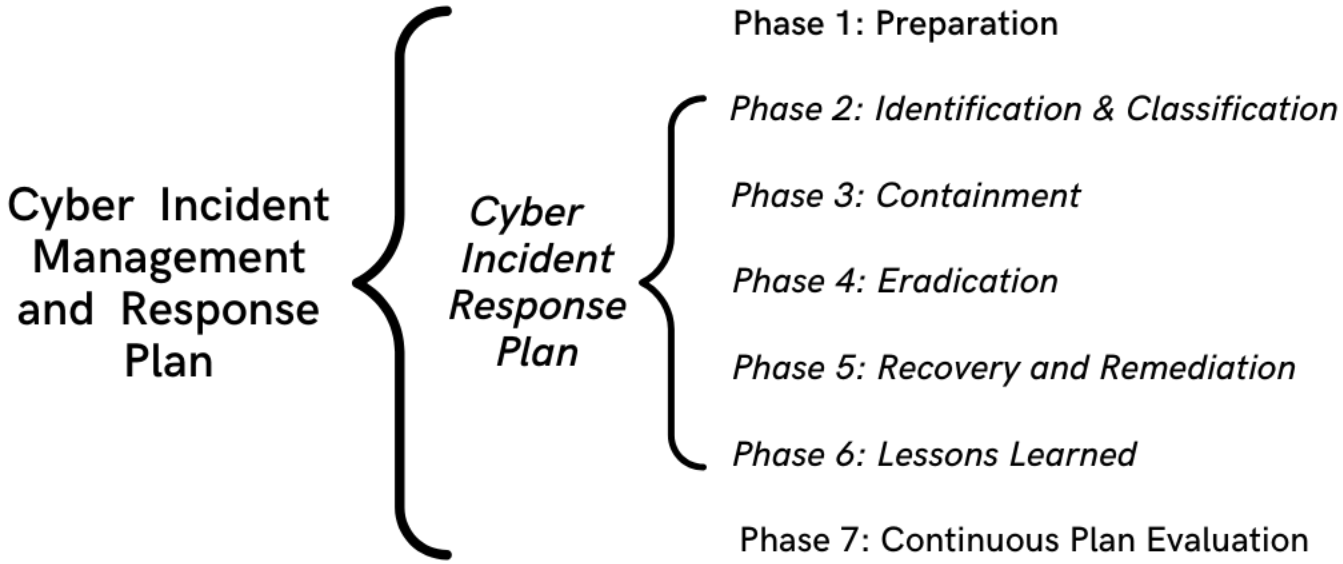
Dustin Glover
State of Louisiana Chief Cyber Officer

AGENDA

- Cyber Incident Management and Response Plan – Organization
- Phase 1 – Preparation
- Phase 2 – Classification and Identification
- Phases 3& 4 – Containment & Eradication
- Phases 5, 6, and 7 - Recovery and Remediation, Lessons Learned, and Continuous Plan Evaluation
- Options for Higher Education
- Options 2 & 3
- Questions
- Key Contact Information

CIMRP Organization

The Cyber Incident Management and Response Plan is a 7 Phase plan, executed in order of the phases.



This model CIMRP is consistent with the State of Louisiana's Information Security Policy.

PHASE 1 - PREPARATION

Identification of Key Personnel:

- **Cyber Steering Group (CSG)**
  - Chief Operations Officer
  - Chief Information Officer
  - Chief Legal Officer
  - Public Relations Officer
- **Cyber Incident Response Manager (CIRM)**
- **Cyber Incident Response Team (CIRP)**
  - Incident Handler
  - Technical or Process Specialists/Representatives
  - Asset Owner
  - Legal/Compliance Personnel
  - Public Relations Representatives

Determine and Document Processes:

- **Cyber Incident Notification Procedures**
  - Internal & External
- **Data Breach Notification Issues**
  - Immediate v. Non-Immediate
  - Legal & CIRT Communications
- **Information Collection Requirements**
  - Minimum requirements: Date/Time, Hostname, Username, Email, Description
  - Cyber Incident Response Report (**CIRR**)
- **Security Event Reporting**
  - Internal & External
  - Indications of Security Event
- **Receipt and Analysis of Security Event**
- **Evidence Collection Process**

PHASE 2 - CLASSIFICATION AND IDENTIFICATION

Identification

Likelihood	Impact				
	Insignificant	Minor	Moderate	Major	Severe
Almost Certain	M	H	H	E	E
Likely	M	M	H	H	E
Possible	L	M	M	H	E
Unlikely	L	M	M	M	H
Rare	L	L	M	M	H

Classification

Post-Classification Actions:

- Begin CIRT assignments
- Cyber Incident Report and Documentation
- Incident Communication

PHASES 3 & 4

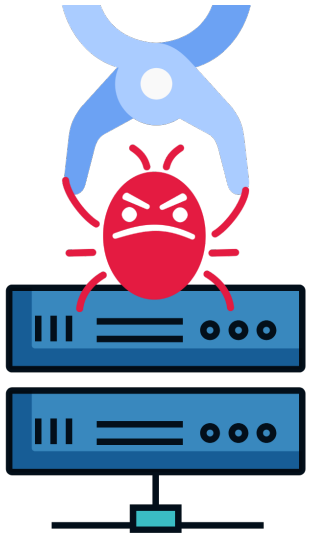
Phase 3 - Containment

- **Short Term Containment**
  - Conduct in a manner to allow contemporaneous root cause analysis.
  - *Example: isolating backups, preventing network traffic.*
- **Root Cause Analysis**
  - Required before long-term containment.
  - No root cause analysis = high chance of ineffective and duplicative efforts; additional cost, redundant labor, and longer/subsequent operational disruptions.
- **Long Term Containment**
  - *Example: cloning an infected system into a quarantined network for analysis and restoring the compromised system to production use.*

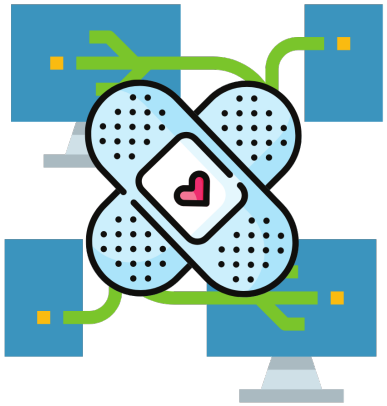
A system cannot be restored to production until completion of the Eradication phase.

Phase 4 - Eradication

- Remove any code, software adaptation, installed application, or system configuration employed by a bad actor or remediate faulty system element
- Examples:
  - *System and Application Patching Resetting, Reconfiguring, or Removing User Accounts, Re-Imaging Compromised Systems or Devices, Improving Network Defenses*



PHASES 5, 6, & 7



Phase 5: Recovery and Remediation:

Restore any impacted technical or operational service and ensure preventative changes are successfully implemented.

- Based on root cause analysis
- Short Term Example: *patch operating systems*
- Long Term Example: *replace firewalls.*

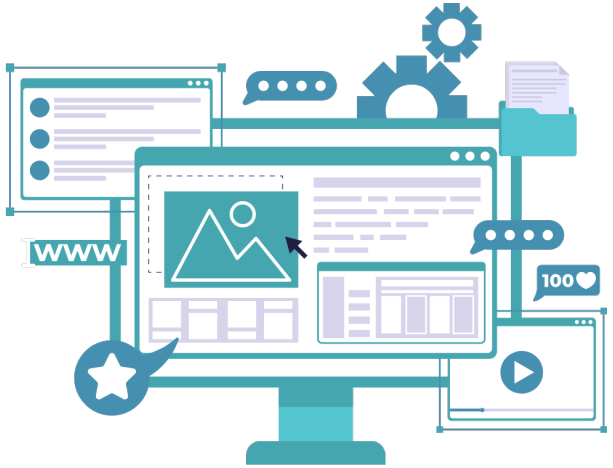
Consult University COOP in event of Complete System Failure.

Phase 6: Lessons Learned

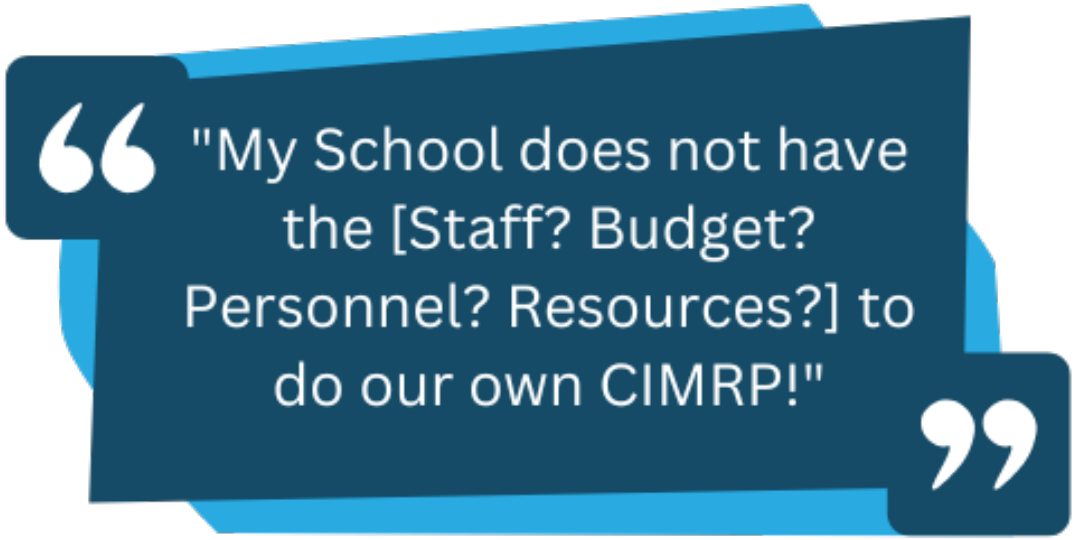
- Why did this happen?
- How do we prevent repeat episode?

Phase 7: Continuous Plan Evaluations

- Conduct training exercises
- Change CIMRP with administrative changes.
- Compare against COOP.



OPTIONS FOR HIGHER-ED



CIMRP OUTSOURCE OPTIONS:

Partial Outsource (option 2):
Utilize Cyber Crime Unit resources for Phases 3 (Containment) and 4 (Eradication).

Full Outsource (option 3):
Utilize ESF-17 (includes CCU) for Cyber Incident Response Plan (Phases 2-6).

All 3 options require University to perform Phase 1 - Preparation

OPTIONS FOR HIGHER-ED

Partial Outsource

CIMRP Phases:

1. University conducts Preparation (notes to call CCU for evidence collection and analysis in plan)
2. University identifies and Classifies Security Event

Once university realizes that the Security Event was ***not a false positive,*** University calls CCU.

3. **CCU & University collaborate for Containment**
4. **CCU & University collaborate for Eradication**
5. University completes Recovery and Remediation
6. University reviews lessons learned
7. University conducts Continuous Plan Evaluation.

CCU collaboration may be onsite or remote – primarily assists with evidence collection, analysis, and root-cause determination.

NOTE: University can request CCU to sample network at any time for analysis – with or without Security Event.

Full Outsource

CIMRP Phases:

1. University conducts Preparation

Once University receives either internal or external report of a security event. CCU will notify remainder of ESF-17 personnel. ESF-17 with University staff and do NOT undertake any action without express consent of University.

2. **ESF-17 & University collaborate for Identification and Classification**
3. **ESF-17 & University collaborate for Containment**
4. ***ESF-17 & University collaborate for Eradication***
5. ***ESF-17 & University collaborate for Recovery and Remediation***
6. ***ESF-17 & University collaborate for Lessons Learned***
7. University conducts Continuous Plan Evaluation.

ESF-17 collaboration may ***stop*** after Phase 4 or ***continue through Phase 6.***

TAKE A VOTE

This is not necessary for me/us.

Self-Completed Full CIMRP
Option 1

Partial Outsource
Option 2

Full Outsource
Option 3

QUESTIONS?

CONTACT INFORMATION

Dustin Glover
Chief Cyber Officer
225.773.6719
Dustin.Glover@la.gov

LTC Stephen Durel
Co-Lead of ESF-17
504.418.0957
Stephen.Durel@la.gov

Corey Bourgeois
OTS Cyber Incident Manager
225.279.4877
Corey.Bourgeois2@la.gov

CMSgt Don Hermann
Infosec Expert
504.237.7841
Don.Hermann@la.gov

Sarah Anderson
ESF-17 Counsel
225.615.0810
Sarah.Anderson@la.gov