



# Beyond “UNPLUG IT, STAT”: Cybersecurity Incident Response Plan Workshop.

Presented by:

Ryan Mulhall, Chief Information Officer  
Iowa Communications Network

# About the ICN

- Business offices are located on Capitol Complex.
- 24 X 7 Network Operations Center (NOC) located at Joint Forces Headquarters (JFHQ) in Johnston.
- 68 full-time staff.



# Celebrating 30 Years of Innovation



## Highlights

- Read Impact Paper
- Discover our History
- Learn Current/Future Projects

[icn.iowa.gov/celebrating30](https://icn.iowa.gov/celebrating30)

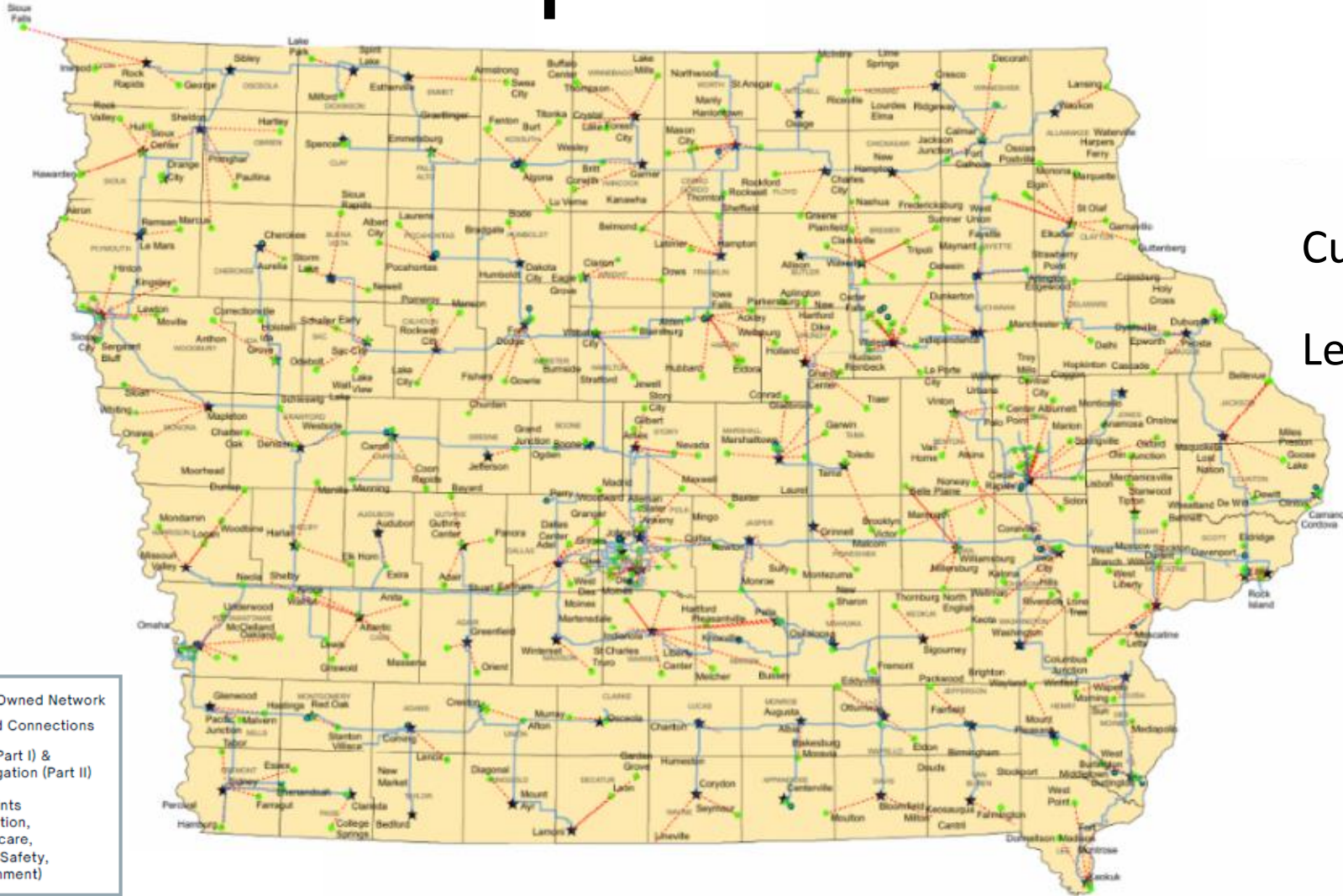
Scan Me



# Services

- Internet
- Ethernet
- Security
  - DDoS Mitigation
  - Firewall
- Cloud Connect
  - AWS / Google / Azure
- Voice
- SIP Transport
- Colocation
- Structured Cabling
- Professional Services

# Network Map



Customer Endpoints  
 -- and --  
 Leased Connections

The Network is approximately **3,400 miles** of owned fiber and leased connections make up the balance.

Connections for services in all **99** counties.

# Customers (Authorized Users)

425+	250+	550+	540+
<b>Education</b>	<b>Healthcare</b>	<b>Government</b>	<b>Public Safety</b>
<b>Locations Served</b> <ul style="list-style-type: none"> <li>• Public &amp; Private K-12</li> <li>• AEAs</li> <li>• Community Colleges</li> <li>• Regents</li> <li>• Private Colleges</li> </ul>	<b>Locations Served</b> <ul style="list-style-type: none"> <li>• Hospitals</li> <li>• Clinics</li> </ul>	<b>Locations Served</b> <ul style="list-style-type: none"> <li>• County Courthouses</li> <li>• DOT Garages, Driver's License Stations, &amp; Construction Offices</li> <li>• DHS Offices</li> <li>• IWD Satellite Offices</li> </ul>	<b>Locations Served</b> <ul style="list-style-type: none"> <li>• PSAPs</li> <li>• Iowa HSEMD</li> <li>• DPS</li> <li>• National Guard</li> </ul>



# State of Iowa Cybersecurity



# What is Cybersecurity?

The art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information.

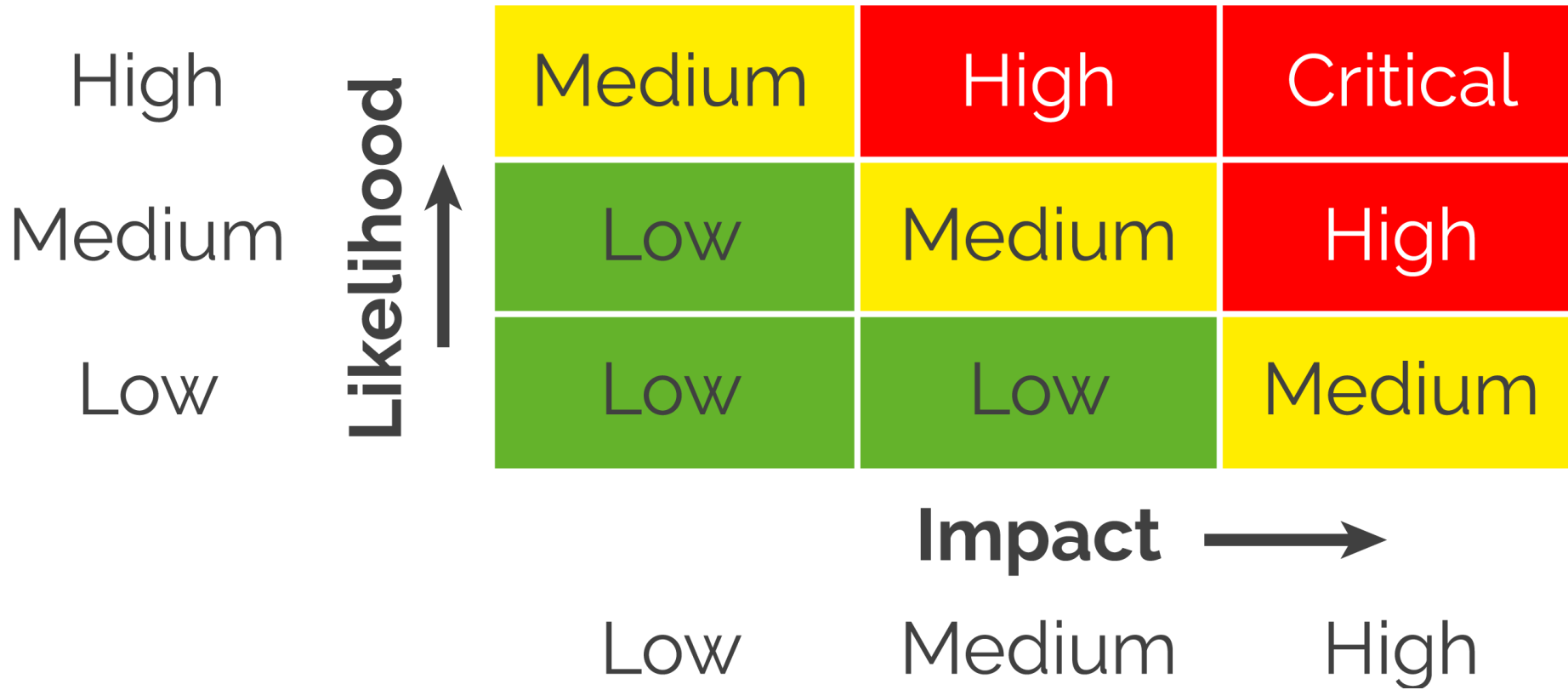
Security = Visibility + Risk



[This Photo](#) by Unknown Author is licensed under [CC BY-SA](#)



# Risk



# Incident Response

Incident Response (IR) is an organized approach to addressing and **managing the aftermath of a security breach or cyberattack**, also known as an IT incident, computer incident, or security incident.

The goal is to handle the situation in a way that limits damage and reduces recovery time and costs.

# Incident Response Resources

- NIST Special Publication 800-61 Revision 2
- Computer Security Incident Handling Guide
- Iowa Code 715C Personal Information Security Breach Protection
- Sample Incident Response Plan/Procedures

# Establishing Capability

- Create an incident response policy and plan
- Develop procedures for performing incident handling and reporting
- Set guidelines for communications with outside parties regarding incidents
- Selection of team structure and staffing model
- Establish relationships between internal and external groups
- Determine what services the IR team should provide
- Staffing and training

# Prevention Still Key

Organizations should reduce the frequency of incidents by effectively securing networks, systems, and applications.

Often less costly and more effective

Incident prevention is complimentary to your IR capability.

# Common Attack Vectors

- External/Removable Media
- Attrition
- Web
- Email
- Improper Usage
- Loss or Theft of Equipment
- Other



# Events vs. Incidents

## Event

Any observable occurrence in a system or network.

## Incident

A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.

# Communications





# Reporting to Law Enforcement

A screenshot of the Federal Bureau of Investigation (FBI) Internet Crime Complaint Center (IC3) website. The page has a blue header with the FBI seal on the left and the IC3 logo on the right. Below the header is a navigation menu with links for Home, File a Complaint, Consumer Alerts, Industry Alerts, and About IC3. The main content area is divided into two columns. The left column features a section titled 'Filing a Complaint with the IC3' with a paragraph of text and a bulleted list of required information. Below this is a red button labeled 'File a Complaint'. The right column has a 'Welcome to the IC3' section with a search bar, followed by a 'Site Navigation' section with links to Alert Archive, FAQs, Disclaimer, Privacy Notice, Internet Crime Prevention Tips, Internet Crime Schemes, and Ransomware. At the bottom of the right column is an 'Annual Report' section with a graphic for the 2019 Internet Crime Report and a link to the 2019 IC3 Annual Report.

**Federal Bureau of Investigation**  
**Internet Crime Complaint Center(IC3)**

[Home](#) [File a Complaint](#) [Consumer Alerts](#) [Industry Alerts](#) [About IC3](#)

### Filing a Complaint with the IC3

The IC3 accepts online Internet crime complaints from either the actual victim or from a third party to the complainant. We can best process your complaint if we receive accurate and complete information from you. Therefore, we request you provide the following information when filing a complaint:

- Victim's name, address, telephone, and email
- Financial transaction information (e.g., account information, transaction date and amount, who received the money)
- Subject's name, address, telephone, email, website, and IP address
- Specific details on how you were victimized
- Email header(s)
- Any other relevant information you believe is necessary to support your complaint

[File a Complaint](#)

### Fraud Alerts

[Consumer Alerts](#) [Industry Alerts](#)

### Welcome to the IC3

### Site Navigation

[Alert Archive](#)  
[FAQs](#)  
[Disclaimer](#)  
[Privacy Notice](#)  
[Internet Crime Prevention Tips](#)  
[Internet Crime Schemes](#)  
[Ransomware](#)

### Annual Report

[2019 Internet Crime Report](#)

2019 IC3 Annual Report

# Incident Handling: Incident Response Lifecycle

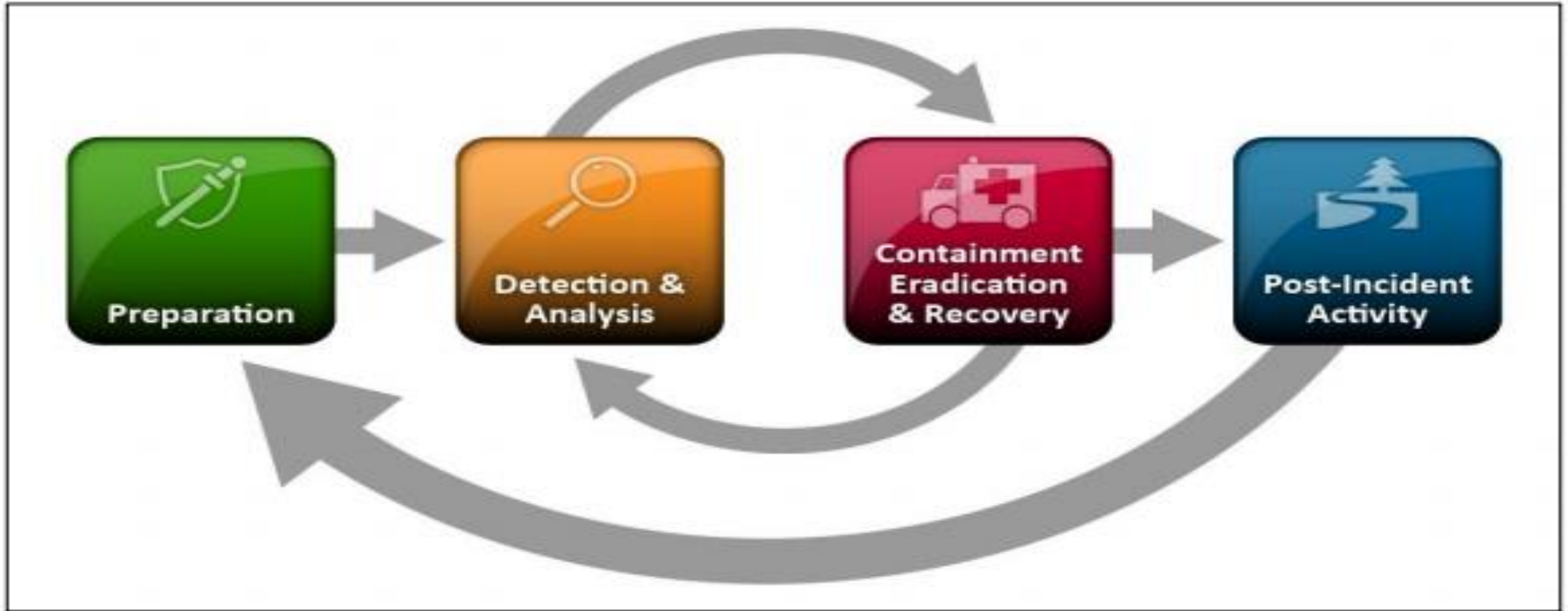


Figure 3-1. Incident Response Life Cycle

# Preparation



# Detection and Analysis

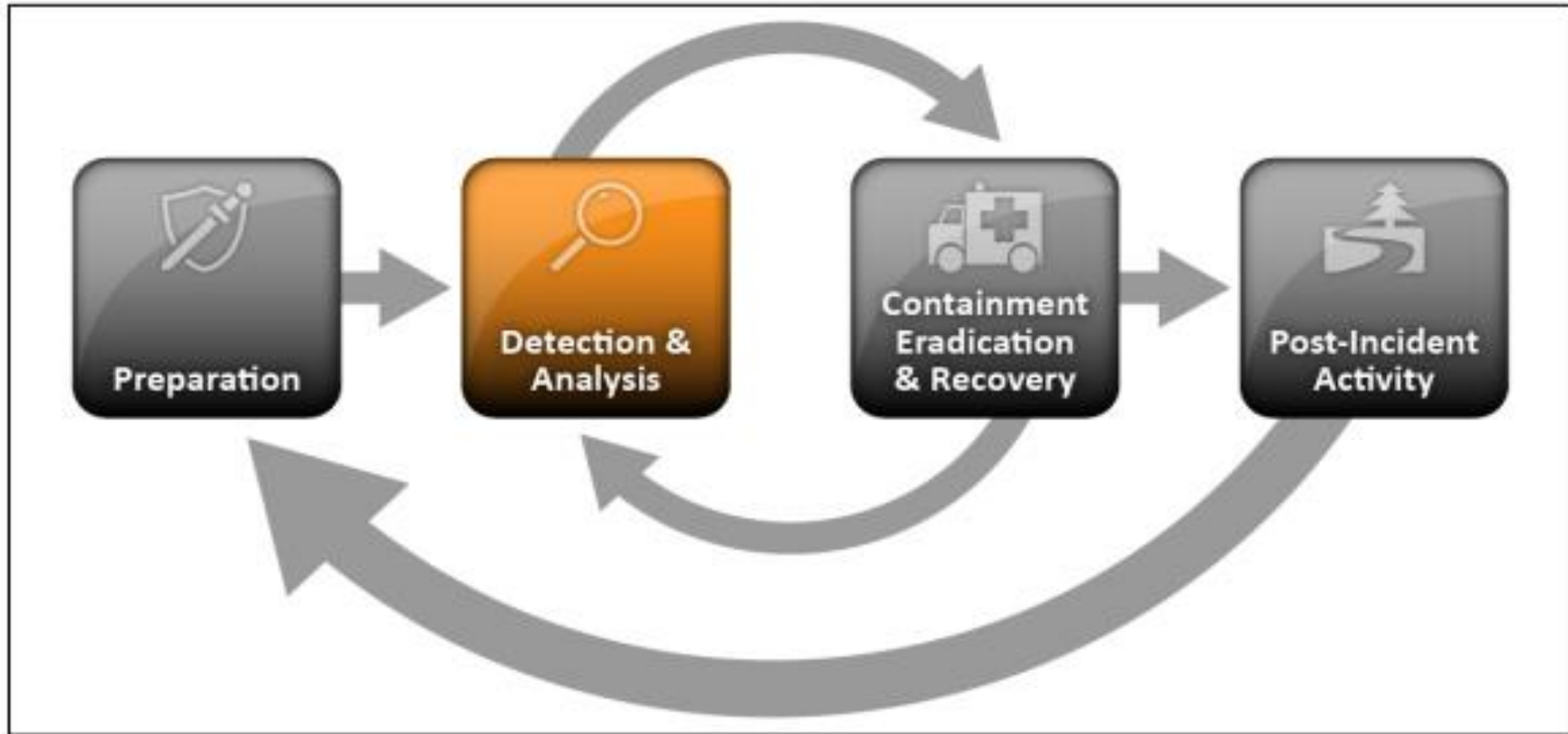


Figure 3-2. Incident Response Life Cycle (Detection and Analysis)

# Incident Documentation

- The current status of the incident (new, in progress, forwarded for investigation, resolved, etc.)
- A summary of the incident
- Indicators related to the incident
- Other incidents related to this incident
- Actions taken by all incident handlers on this incident
- Chain of custody, if applicable
- Impact assessments related to the incident
- Contact information for other involved parties (e.g., system owners, system administrators) ☒
- A list of evidence gathered during the incident investigation
- Comments from incident handlers
- Next steps to be taken (e.g., rebuild the host, upgrade an application).

# Incident Prioritization

Functional Impact of the Incident

Information Impact of the Incident

Recoverability from the Incident

# Incident Notification

- CIO – Other Executives
- Head of information security
- Local information security officer
- Other incident response teams within the organization
- External incident response teams (if appropriate)
- System owner
- Human resources (for cases involving employees, such as harassment through email)
- Public affairs (for incidents that may generate publicity)
- Legal department (for incidents with potential legal ramifications)
- Law enforcement (if appropriate)

# Containment, Eradication, Recovery

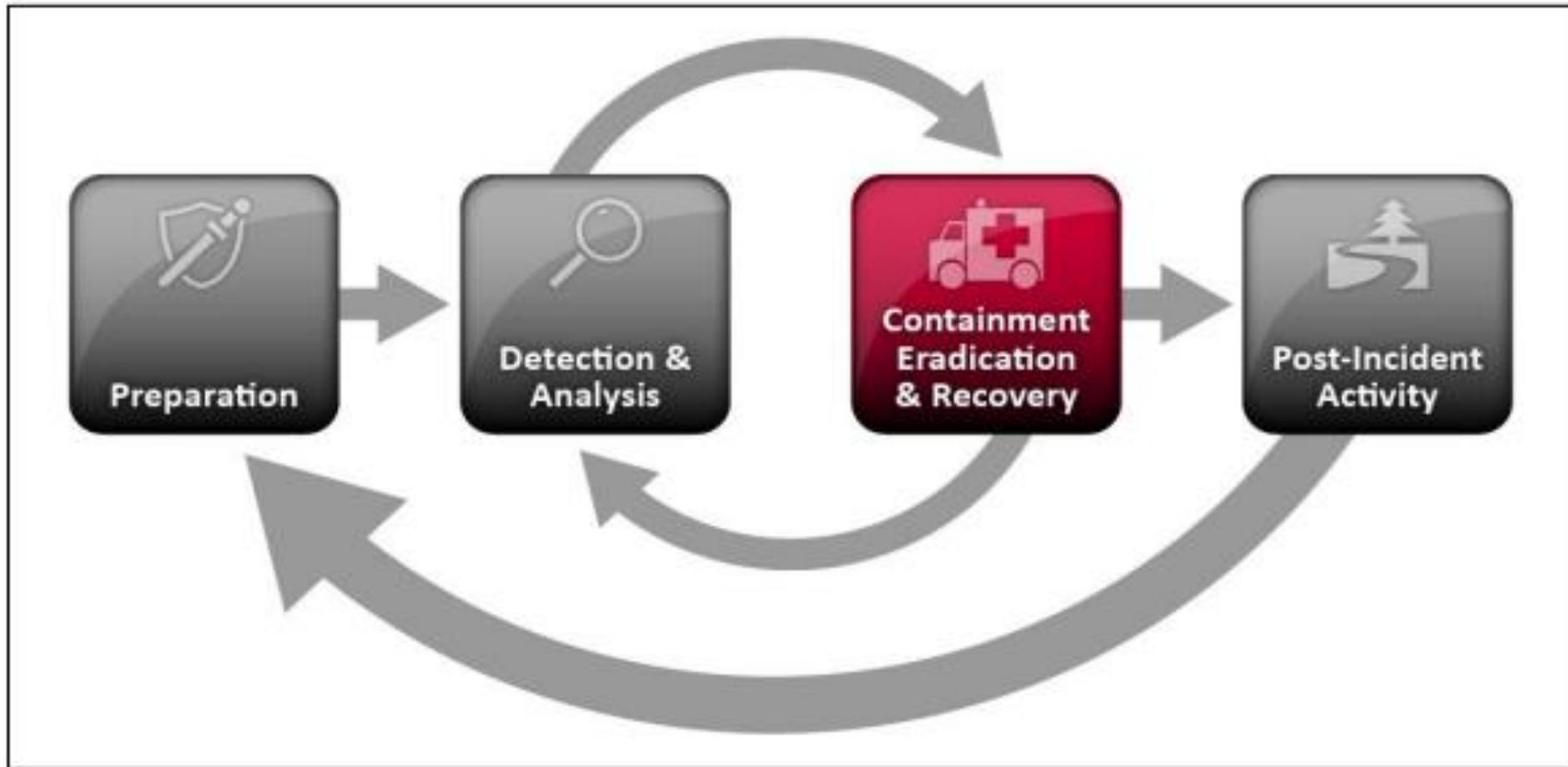
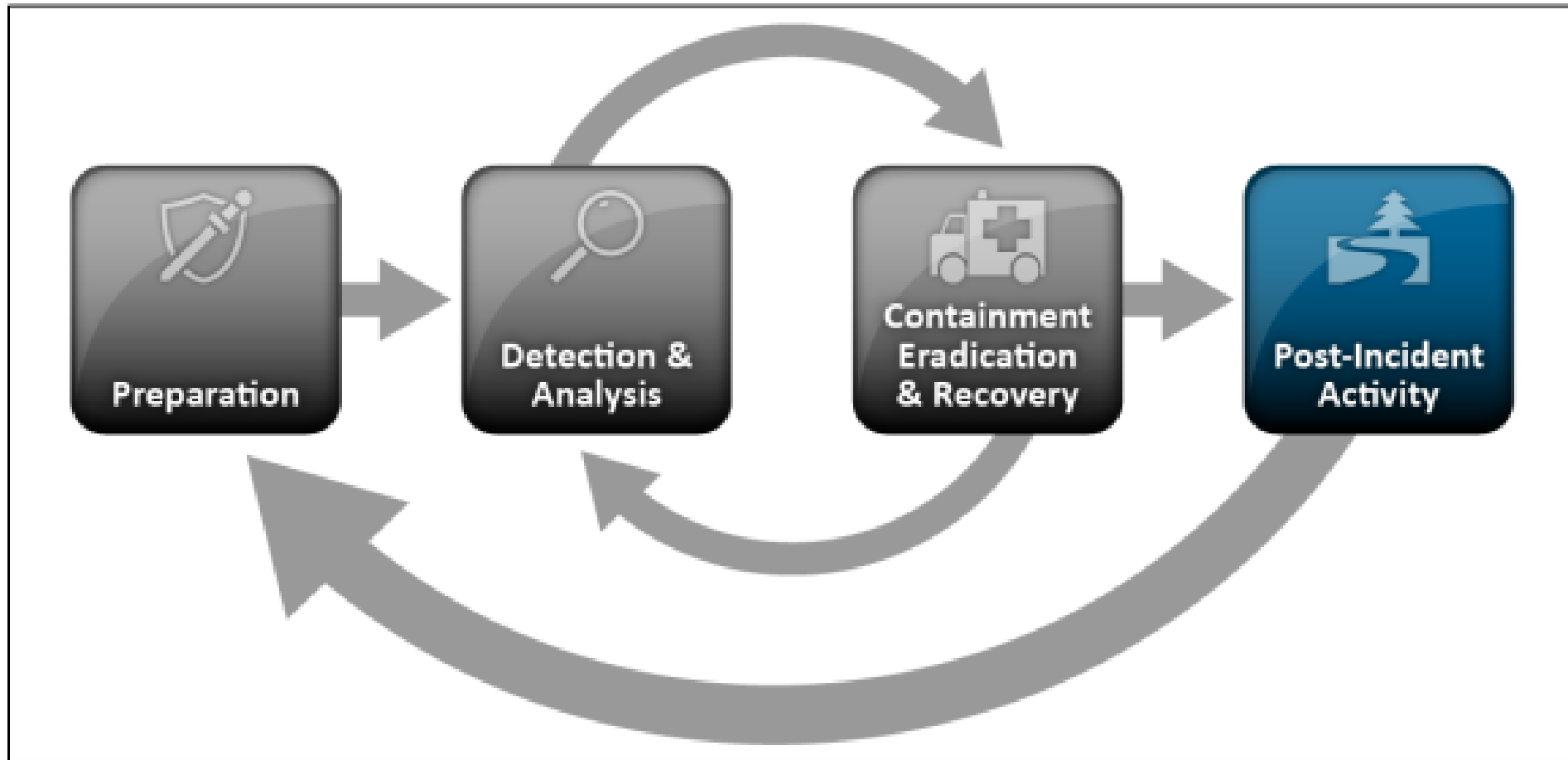


Figure 3-3. Incident Response Life Cycle (Containment, Eradication, and Recovery)



# Post Incident Activity



**Figure 3-4. Incident Response Life Cycle (Post-Incident Activity)**

# Collected Data and Metrics

Number of Incidents Handled

Time Per Incident

Objective Assessment of Each Incident

Subjective Assessment of Each Incident

# Sample Incident Response Plan/Procedures

## SAMPLE INCIDENT RESPONSE PLAN/PROCEDURES

*\*Note: Change highlighted areas to specific information related to your organization to tailor the PLAN/PROCEDURES for a quick, easy plan.*

- 1) Any individual who discovers the indicators of a cyber security incident will notify **Notified Entity**.
- 2) **Notified Entity** will provide an initial analysis by documenting responses to the following questions as they pertain to affected **information systems/assets**.
  - a) Please summarize the incident?
  - b) How was the incident discovered?
    - a) Names of systems being targeted, along with operating system, IP addresses, and locations.
    - b) IP address and any information about the origin of the attack.

(1) What Personally Identifiable Information (PII) or Protected Health Information (PHI) is known or suspected to be involved?

  - A) Information that can be documented in our systems
    - 1) Names
    - 2) Usernames
  - B) Only the type of Information can be documented in our systems

# Questions



## Statewide Youth Broadband Advisory Council

- Established in 2015.
- Great Experience for High School Students.
- Cybersecurity Certification.
- Hear from Industry Leaders.
- Learn About Technology Happening in Iowa.
- Network with Peers.



[icn.iowa.gov/sybac](https://icn.iowa.gov/sybac)

**Now taking applications for 2023/24 school year.**




Scan to Connect  
with the ICN



# Thank You.

*Contact us for more information or to  
schedule a tour of our Network facilities.*

 Ryan Mulhall

 515-725-8920

 [ryan.mulhall@icn.state.ia.us](mailto:ryan.mulhall@icn.state.ia.us)

 [icn.iowa.gov](http://icn.iowa.gov)