Incident Response Planning

Mat Wilcek, CISSP, PCI-QSA
Information Security Manager

CliftonLarsonAllen

cliftonlarsonallen.com

Agenda

- Purpose of an IR Plan
- Elements of an Incident Response (IR) Plan
- Creating and Implementing an IR Plan
- IR Team
- Best Practices for an IR

Who am I?

Current

- CliftonLarsonAllen
  - Help State and Local Government, Non-Profit Organizations, Credit Unions, and Banks Assess Their (Information) Security

Past

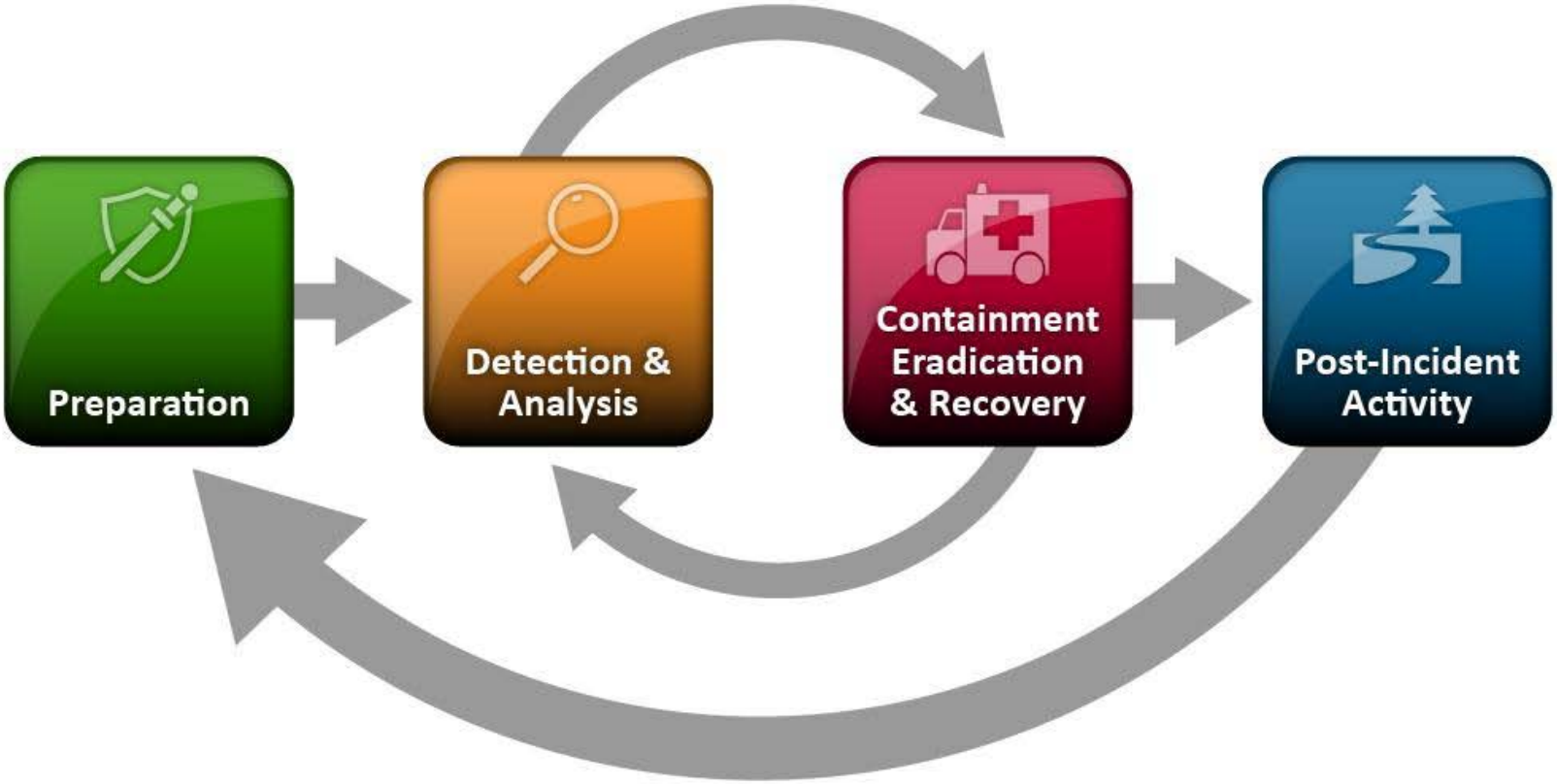
- Chief Information Security Officer (CISO) at MN State Agency
- Consultant (Network Security)
- Network Security Engineer at MN County

Purpose of an Incident Response plan

Purpose

- Prepare for Unscheduled Computer Incidents
- Identify Potential Threats and Vulnerabilities
- Develop Best Responses and Reduce Damage
- Apply Critical Thinking to Solve Problems

Purpose



Incident Response Life Cycle

Purpose

- How can an IR Plan Mitigate Risk?
  - Quick and Focused Response to Incidents
  - Clearly Defined Roles and Responsibilities for Response
  - Enhanced Understanding of Needed Skills
  - Enhanced Understanding of Needed Controls, Processes, and Technology
  - Enhanced Ability to Respond to Threats and Remove Risks

Elements of an Incident Response Plan

Elements

- Mission
- Strategies and goals
- Senior management approval
  - Members of the Response Team
  - Accountabilities
  - Policies
  - Procedures
  - Communication Escalation Procedures

Elements

- Organizational approach to incident response
- How the incident response team will communicate with the rest of the organization and with other organizations
- Metrics for measuring the incident response capability
- Roadmap for maturing the incident response capability
- How the program fits into the overall organization

Elements (Communications)

Elements (Communications)

- Employees/Internal Personnel
- The Media
- Law Enforcement
  - FBI
  - US Secret Service
  - District Attorney/State & Local Law Enforcement
- Incident Reporting Organizations

Creation and Implementation

Creation and Implementation

Phase 1: Preparation

- Determine the scope of the incident response process.
- Create an incident taxonomy
- Assign roles and responsibilities
- Establish a single point of command for the response team.

Phase 2: Detection & Analysis

- Identify detection channels
- Determine severity of incidents and prioritize response.
- Designate response timelines by severity level.

Phase 3: Containment, Eradication, and Recovery

- Develop a clear response process.
- Engage the incident response team to remediate the problem.
- Balance the need for recovery with forensic evidence preservation.
- Determine when and how to communicate with employees, media, customers, and law enforcement.

Phase 4: Post-Incident Improvement

- Conduct postmortem conversations.
- Track incident data and metrics.
- Measure incident response team performance.
- Drive security improvements based on learnings from incidents.
- Train

Creation and Implementation

Phase 1: Preparation

- Determine the scope of the incident response process.
- Create an incident taxonomy.
- Assign roles and responsibilities.
- Establish a single point of command for the response team.

Creation and Implementation

Phase 2: Detection & Analysis

- Identify detection channels.
- Determine severity of incidents and prioritize response.
- Designate response timelines by severity level.

Creation and Implementation

Phase 3: Containment, Eradication, and Recovery

- Develop a clear response process.
- Engage the incident response team to remediate the problem.
- Balance the need for recovery with forensic evidence preservation.
- Determine when and how to communicate with employees, media, customers, and law enforcement.

Creation and Implementation

Phase 4: Post-Incident Improvement

- Conduct postmortem conversations.
- Track incident data and metrics.
- Measure incident response team performance.
- Drive security improvements based on learning's from incidents.
- Train.

Members

Members

- Team Leader (Information Security/Privacy Officer)
  - Information Security Personnel
- IT Department
  - Server, Network, Database Administrators
- Physical Security
- Internal Audit
- Legal Counsel
- Human Resources
- Communications/PR Personnel
- External Response Capabilities (IR Support/Forensics)

Best Practices

Best Practices

- Define what a security incident is
- Develop and include policies in the plan to guide members and employees
- Provide training
- Develop checklists
- Develop Metrics to Evaluate Effectiveness
- Subscribe to Security Notification Bulletins
- Lessons Learned Exercises

Summary

- Purpose of an IR Plan
- Elements of an Incident Response (IR) Plan
- Creating and Implementing an IR Plan
- IR Team
- Best Practices for an IR

Resources

- Anti-Phishing Working Group (APWG)
  http://www.antiphishing.org/
- Computer Crime and Intellectual Property Section (CCIPS), U.S. Department of Justice
  http://www.cybercrime.gov/
- CERT® Coordination Center, Carnegie Mellon University (CERT®/CC)
  http://www.cert.org/
- Forum of Incident Response and Security Teams (FIRST)
  http://www.first.org/

Resources

- Government Forum of Incident Response and Security Teams (GFIRST)

  http://www.us-cert.gov/federal/gfirst.html
- High Technology Crime Investigation Association (HTCIA)

  http://www.htcia.org/
- Internet Storm Center (ISC)

  http://isc.incidents.org/
- United States Computer Emergency Response Team (US-CERT)

  http://www.us-cert.gov/

NIST Publications

NIST SP 800-53 Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*
http://csrc.nist.gov/publications/PubsSPs.html#800-53

NIST SP 800-83, *Guide to Malware Incident Prevention and Handling*
http://csrc.nist.gov/publications/PubsSPs.html#800-83

NIST SP 800-84, *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*
http://csrc.nist.gov/publications/PubsSPs.html#800-84

NIST SP 800-86, *Guide to Integrating Forensic Techniques into Incident Response*
http://csrc.nist.gov/publications/PubsSPs.html#800-86

NIST SP 800-92, *Guide to Computer Security Log Management*
http://csrc.nist.gov/publications/PubsSPs.html#800-92

NIST SP 800-94, *Guide to Intrusion Detection and Prevention Systems (IDPS)*
http://csrc.nist.gov/publications/PubsSPs.html#800-94

NIST SP 800-115, *Technical Guide to Information Security Testing and Assessment*
http://csrc.nist.gov/publications/PubsSPs.html#800-115

NIST SP 800-128, *Guide for Security-Focused Configuration Management of Information Systems* http://csrc.nist.gov/publications/PubsSPs.html#800-128

References

Information Risk Executive Council, *Developing a Systematic Incident Response Program*

NIST SP 800-61 Revision 2, *Computer Security Incident Handling Guide*

2012 Verizon Data Breach Investigations Report

http://www.verizonenterprise.com/DBIR/2012/