PLANNING EXECUTIVE RESPONSE TO CYBER SECURITY INCIDENTS

Luis Tapia, Sr. Business Continuity Analyst

Paloma Alaniz, Business Continuity Analyst

October 13, 2016


COMPUTER
CYBER
SYSTEM
INFORMATION
SECURE
OPERATING
NATIONAL
SYSTEMS
SECURITY
ACCESS
DATA
SOFTWARE
CYBERSECURITY
ONE
COMMON
VULNERABILITIES
DESIGN
PROTECTION
DEFECTS
DEFENSE
POWER
LEVEL
WELL
LOSS
INTERNATIONAL
COMPROMISED
PROTECTING
HOUSE
INCLUDE
SERVICES
PRIMARY
COMPUTERS
BILL
PROTECT
BASED
USED
STATES
NEW
SITE
INTRUSION
TECHNOLOGY
ASSURANCE
MAIN
INFRASTRUCTURE
MANAGEMENT
INTERNET
FLAWS
ORDER
PROVIDE
NETWORK
UNITED
MANY
ACT
IMPLEMENTED
AIR
ISSUES
LEVELS
LEGAL
WORLD
PROBLEM
ENSURE
CODE
HIGH
USING
CENTER
SEGMENTS
CODING
TECHNIQUES
USE
COMMUNICATIONS
NEEDED
APPLICATION
CAPABILITIES
ATTACK
CONTROL
HARDWARE
FILES
ENGINEERING
ARTICLE
ANOTHER
NETWORKS
DESIGNED
KNOWN
CRITICAL
CYBERCRIME
CONNECTED
POLICY
GOVERNMENT


SIGNIFICANT
INFORMATION
TAMPERING
STOCK
RECOVERY
DETECTION
MISDEEDS
CONTINGENCY
PRECIPITATOR
MISREPRESENTS
COMPETENCY
SECTOR
CATASTROPHE
MISCONDUCT
REPUTATIONAL
OFFICIAL
COLI
ORGANIZATION
CAUSED
CRISIS
GRISLY
LEADERSHIP
CRISES
SKEWED
THREAT
DECEPTION
NEWS
BLAMED
VALUES
MEMBERS
STAGE
AMORALITY
LEADER
DAMAGE
MANAGEMENT
CONTINUITY
MANAGEMENT
MALEVOLENCE
APOLOGY
SOCIAL
MEDIA
MAKING
FORESHADOWED
STAKEHOLDER
RELATIONS
HUMAN
INNOVATION
CRISIS
HANDLERS
ORGANIZATIONAL
REPUTATION
PHASE
DISASTER

HOW TO ACHIEVE READINESS

Goal: Enhance executive readiness for cyber security incidents

Involves actions required to execute a wide range of incident management activities

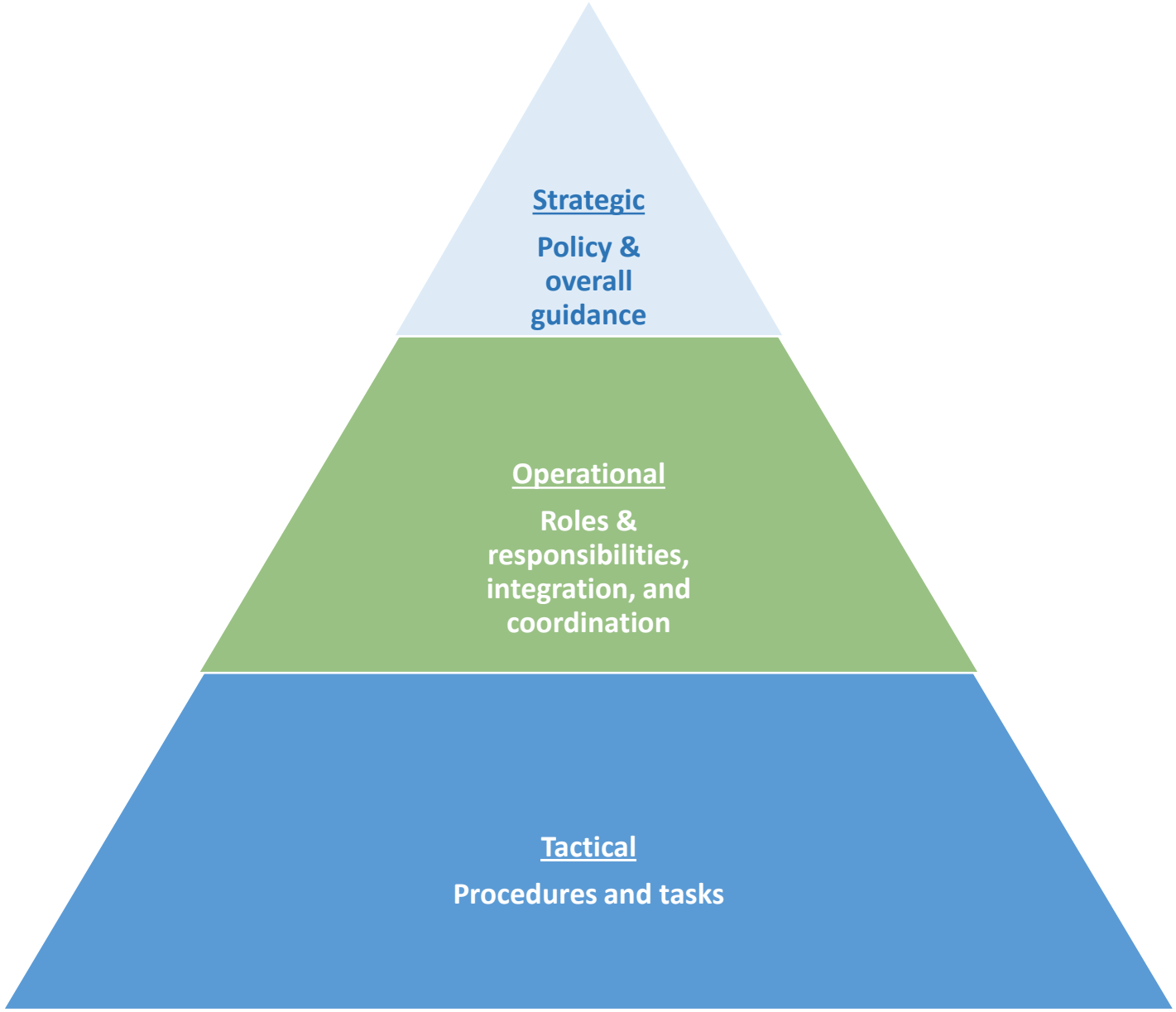
Continuous cycle of planning, organizing, training, exercising, and improvement

TYPES OF DOCUMENTS

Information Security Policy

Executive Cyber Security Incident Response Plan

Incident Handling Procedures



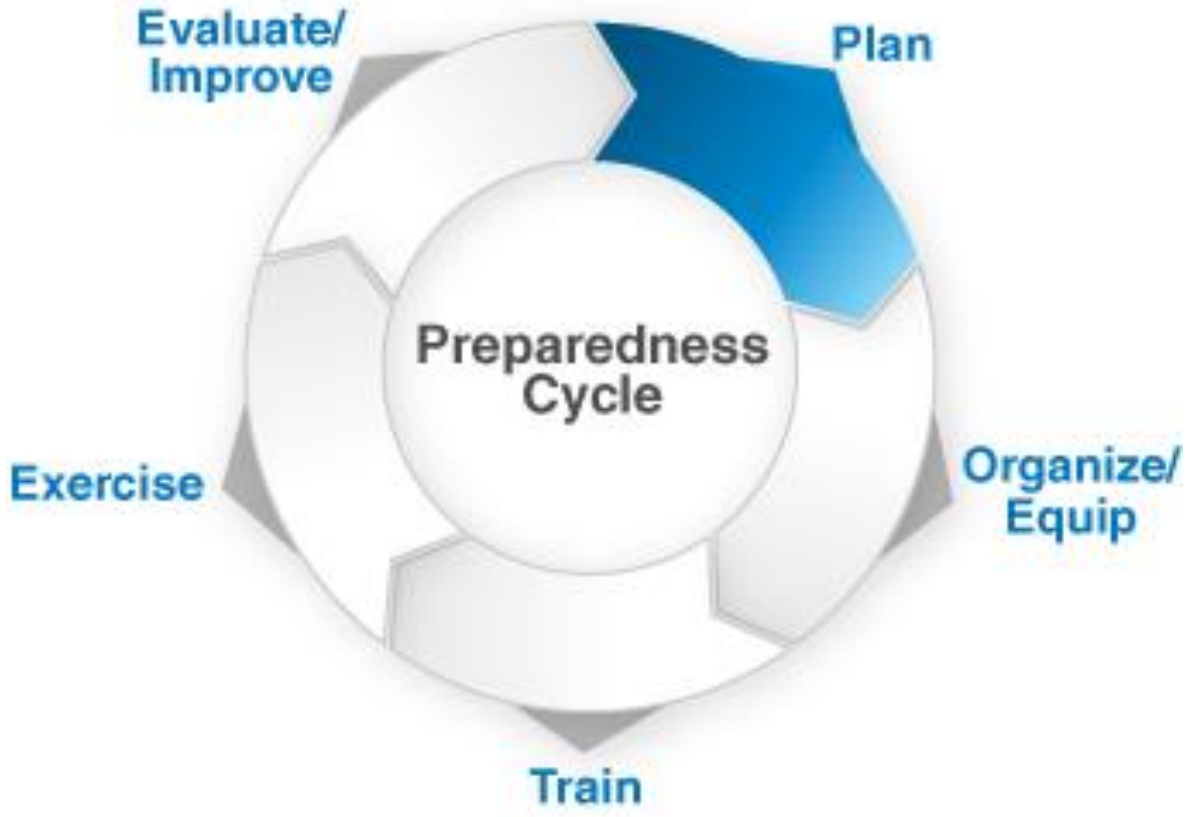
EXECUTIVE CYBER SECURITY INCIDENT RESPONSE PLAN

Questions Plans Address:

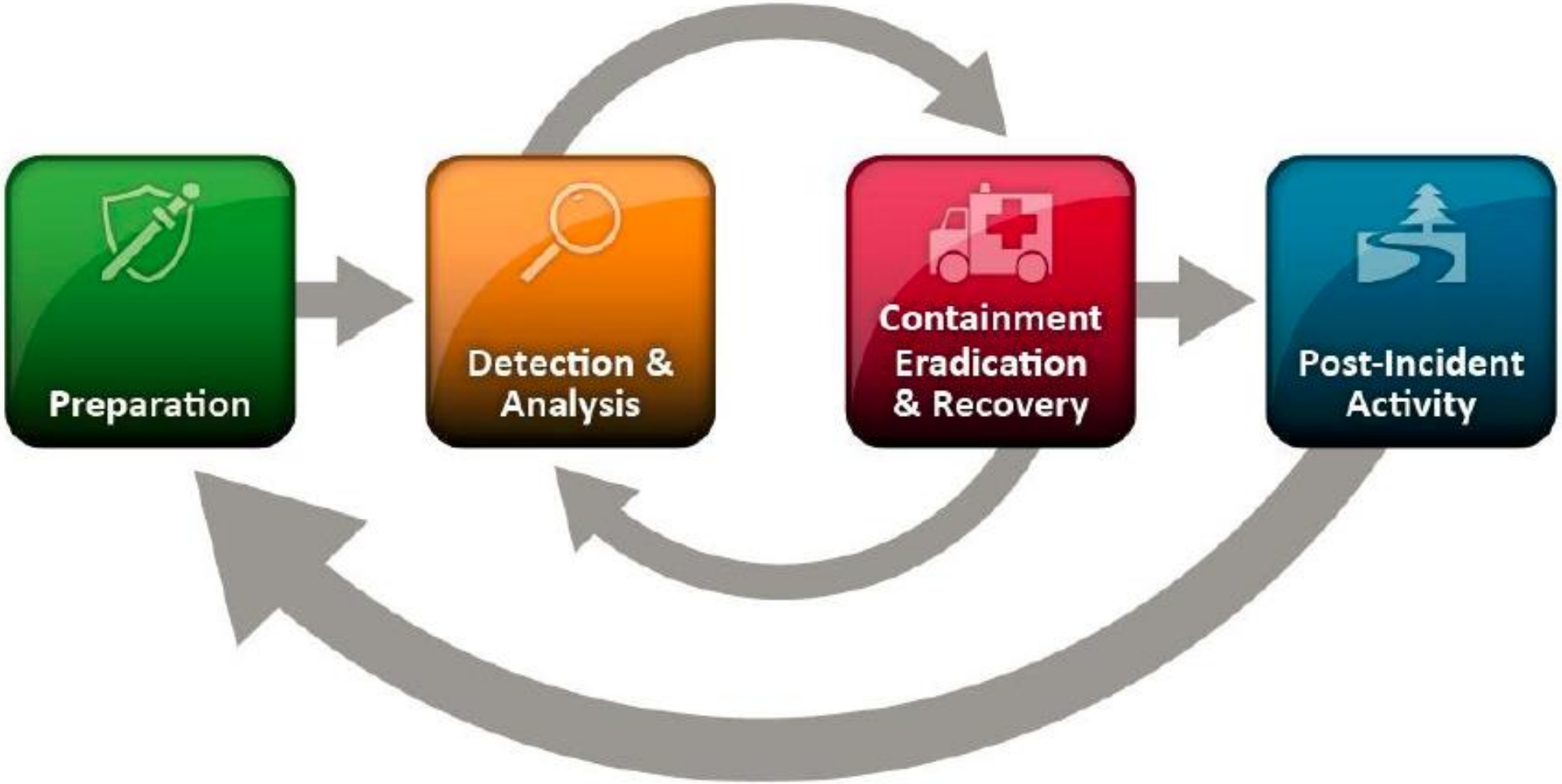
- Who is involved?
- What do they do?
- When do they do it?

Capabilities Plans Enable:

- Information Sharing
- Coordination
- Communication



INCIDENT RESPONSE LIFE CYCLE



ORGANIZING RESOURCES

Crucial Resources:

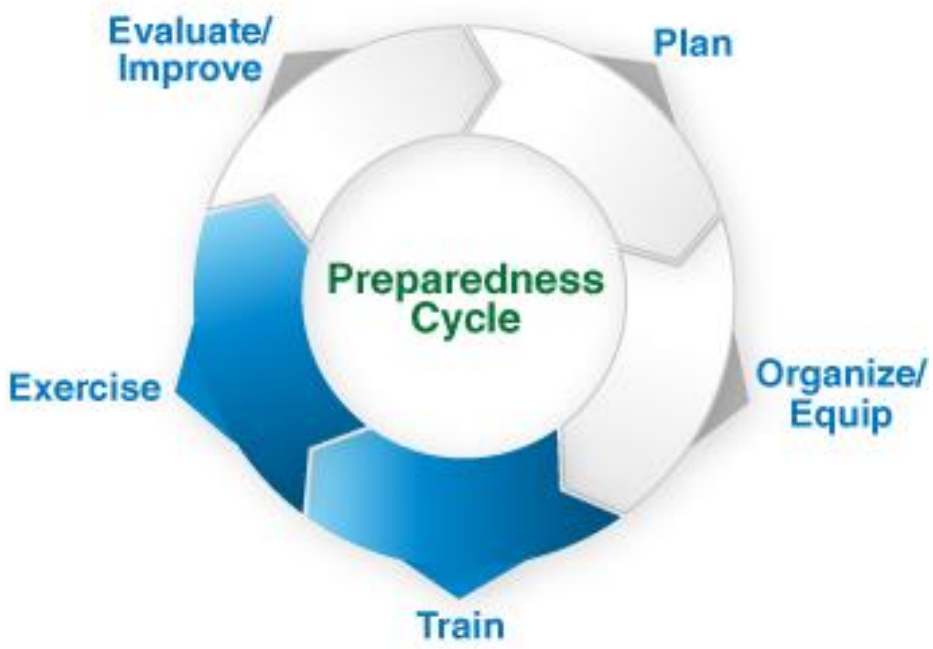
- Subject Matter Experts
- War Room
- Cost Centers
- Contracts
- Agreements
- Contact Lists (Internal/External)
- Other Vital Records
- Secure Conference Bridge

TRAINING AND EXERCISING

Goal: Build muscle memory by practicing processes and use of resources

Benefits Include:

- Evaluate plans
- Reinforce teamwork
- Clarify roles
- Pinpoint resource gaps
- Eliminating “stovepipes”



TYPES OF EXERCISES

Exercise Types

- Seminars
- Workshops
- Tabletops
- Drills

Exercise Focus:

- End to end
- Single area
- Capability

EXERCISE CONSIDERATIONS

Availability

Scope, Objectives, and Requirements

Scenario

Rules, Assumptions and Artificialities

Facilitation

Exercise Support Personnel and Participants

Wrap-up Activities

Measuring Performance

AFTER ACTION REPORT / IMPROVEMENT PLAN

Evaluation Process

- Select evaluator
- Define evaluation requirements
- Observe exercise
- Collect data
- Analyze data
- Identify corrective actions
- Complete report
- Track remediation

CONTACT US

Luis Tapia

- ltapia4@jcp.com

Paloma Alaniz

- pgarci37@jcp.com