

Information Security Incident Response

Sharvind Appiah
Assistant Manager
CERT-MU

Agenda

- Definitions
- Need for Incident Response
- Incident Response Process
- Incident Response Lifecycle
- CERT-MU



National Computer Board



CERT-MU

Definitions

- Event v/s Incident
- What is an Information Security Incident?
- Evolution of the concept

“The art of war teaches us to rely not on the likelihood of the enemy's not coming and on the chance of his not attacking, but on our own readiness to receive him.” – Sun Tzu



National Computer Board



CERT-MU

Need for Incident Response

- Increased frequency of external attacks
 - 114,000 incidents in 9 months – CERT/CC
 - 451 incidents in 1st quarter - HKCERT
- Increased frequency of insider threats
 - 2009 – Year of the Insider Threat
- Organized high tech crime
 - Growing underground economy
- Increased impacts of incidents
 - Financial and non financial loss



National Computer Board



CERT-MU

Incident Response Process

- 4 stages
 - Preparation
 - Detection & Analysis
 - Containment, Eradication & Recovery
 - Post-Incident Analysis
- Incident Response Lifecycle

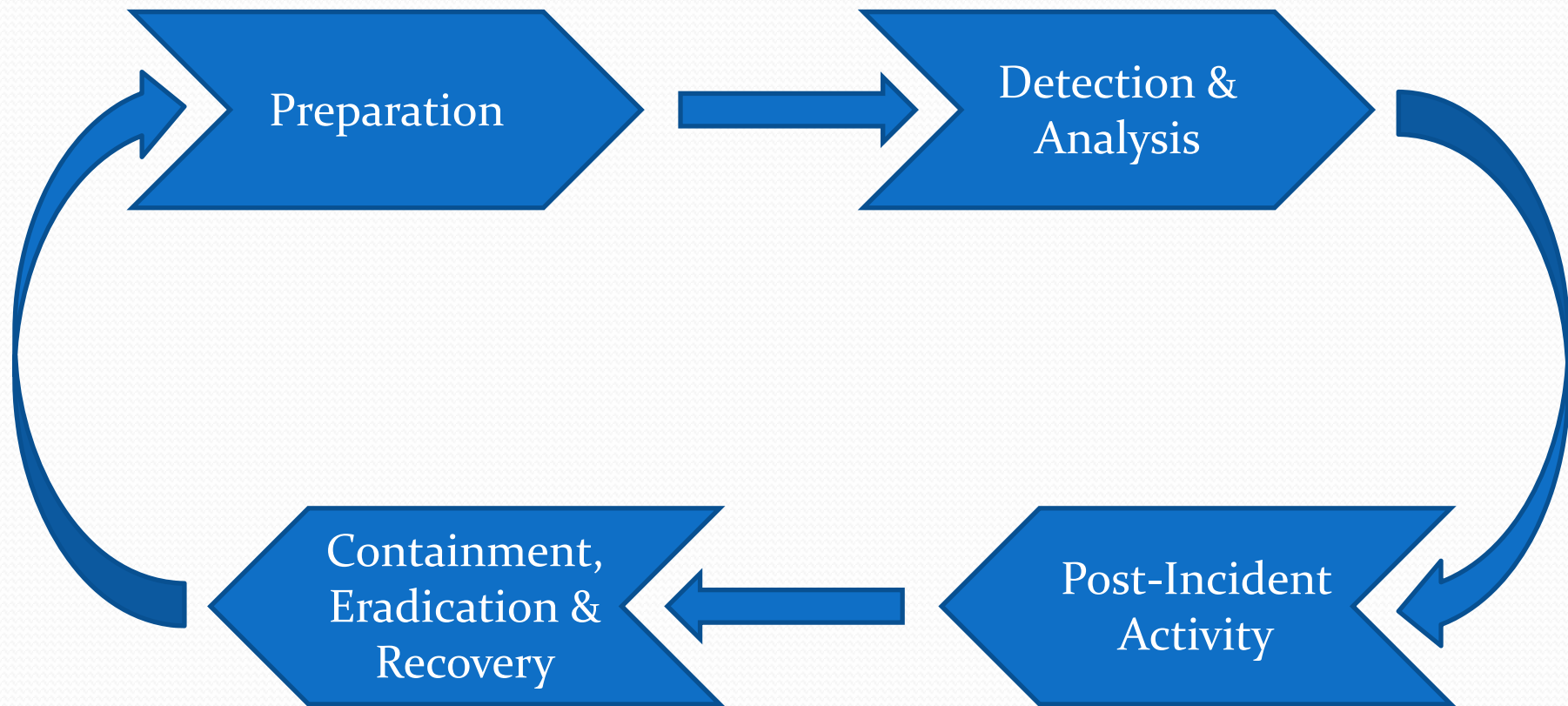


National Computer Board



CERT-MU

Incident Response Lifecycle



National Computer Board



CERT-MU

Preparation Stage - I

- Preparation to avoid incidents
 - Policies & Procedures
 - Host Security
 - Patch Management
 - Network Security
 - Malicious Code Prevention
 - Awareness and Training



National Computer Board



CERT-MU

Preparation Stage - II

- Preparation to manage incidents
 - Establish incident handling capability
 - Communications and Facilities
 - Hardware and Software
 - Analysis Resources
 - Recovery Procedures
 - Mitigation Strategies and Tools



National Computer Board



CERT-MU

Detection and Analysis - I

- Classification and Categories
 - DOS, Misuse, Malicious Codes
- Precursors and Indications
 - Server Crashes, Unusual Activities
- Sources of Precursors and Indications
 - IDS, Server Logs, Honeypot Logs



National Computer Board



CERT-MU

Detection and Analysis - II

- Profiling Networks and Systems
- Understand “Normal” behavior
- Centralized Logging and Retention
- Maintain a Knowledge Base
- Filtering Precursors Data
- Maintain a Diagnosis Matrix
- Documentation & Records
- Incident Prioritization
- Notification Procedure



National Computer Board



CERT-MU

Containment & Recovery

- Containment Strategy
 - Impact, Resources, Recovery Time
- Evidence Gathering and Handling
 - Location, Chain of Custody, Documentation
- Identify the source or attacker
 - IP address, Attack System, Database, Communications
- Eradication
 - Normal operations, delete compromised data.



National Computer Board



CERT-MU

Post-Incident Activity

- Lessons Learned
 - Why? What? How? When?
 - Improvement
 - Effectiveness of Strategies
- Collected Incident Data
 - Number of Incidents, Objective assessment, Subjective Assessment
- Evidence Retention
 - Prosecution, Data Retention, Costs



National Computer Board



CERT-MU

Incidents reported to CERT-MU

- Local sources
 - ISPs
 - Law enforcement Agencies
 - Regulatory Bodies
- International Sources
 - International CERTS
 - Country Agencies



National Computer Board



CERT-MU

Conclusion

- Incident Response is quintessential
- Continuous Adaptive Process
- Rapid Evolution

“In security, the past is no guarantee, the present is not perfect and the future is uncertain.”



National Computer Board



CERT-MU



THANK YOU



National Computer Board



CERT-MU