SETTING UP A COMPUTER EMERGENCY RESPONSE TEAM (CERT)

Alwell C. Mulsid
Philippine National CERT (CERT-PH)

OBJECTIVES

- To understand why we need to setup a CERT in our organization
- To know the requirements on how to setup a CERT
- Define what CERT services the organization should have
- To know the roles, responsibilities and access of the team

DICT
DEPARTMENT OF INFORMATION AND COMMUNICATIONS TECHNOLOGY

OBJECTIVES

- To understand and adapt the best practices in creating a CERT.

- Understand the CORE Principles of CERT

- Scenario based exercise

hy d

The entire IT landscape has changed. Cyberspace became a one top shop for services, information and businesses.

A. Increase in the number of computer security incidents being reported

B. Increase in the number and type of organizations being affected by computer security incidents

hy d

C. Security policies and standard practices as part of organization's overall risk-management strategies

D. New laws and regulations that impact how organizations are required to protect information assets

hy c

E. Realization that IT, Systems engineers and network administrators cannot protect organizational systems and assets

F. With the internet connectivity and Internet of Things an organization should defend from global attacks

A. Ask authorization and obtain management support

- To ensure the success of the creation and implementation of CERT top management support is very important.

- authority must come from board/CEO/Department Secretary (not from IT HEAD)

- Do it in a letter form with approval.

B. Determine the CERT strategic plan

- CERT Strategic plan should be placed into writing as this will be used to move the organization from its current security state to a future security state where assessed security gaps are being addressed, and new services deployed.

C. Gather relevant information

- Gather information on what is the current technology and application portfolio, current business plans, and then gain an understanding of the critical data types required by the stakeholders.

st

D. Design the CERT vision

- A trusted confidant partner in responding to Cyber Security incidents.

- Incorporate a continuous security mindset into all aspects of organization functions.

st

DICT
DEPARTMENT OF INFORMATION AND COMMUNICATIONS TECHNOLOGY

E. Communicate the CERT vision and operational plan

F. Begin CERT implementation

G. Announce that the CERT is operational

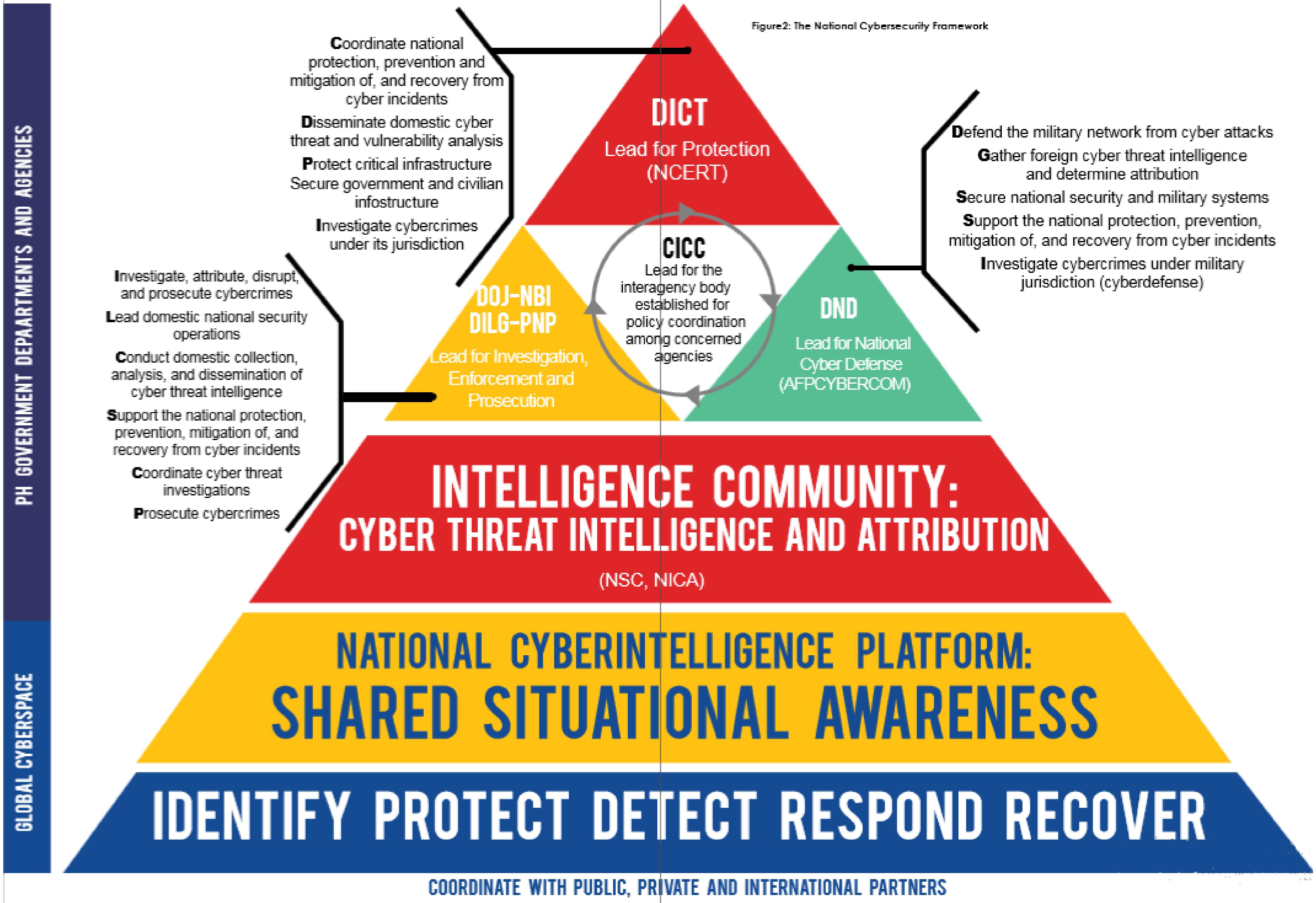
H. Evaluate CERT effectiveness

ttin

A. Requirements in establishing a CERT

- Design your CERT Framework

Figure2: The National Cybersecurity Framework



PH GOVERNMENT DEPARTMENTS AND AGENCIES

GLOBAL CYBERSPACE

DICT

Lead for Protection (NCERT)

Coordinate national protection, prevention and mitigation of, and recovery from cyber incidents

Disseminate domestic cyber threat and vulnerability analysis

Protect critical infrastructure

Secure government and civilian infostructure

Investigate cybercrimes under its jurisdiction

CICC

Lead for the interagency body established for policy coordination among concerned agencies

DOJ-NBI DILG-PNP

Lead for Investigation, Enforcement and Prosecution

Investigate, attribute, disrupt, and prosecute cybercrimes

Lead domestic national security operations

Conduct domestic collection, analysis, and dissemination of cyber threat intelligence

Support the national protection, prevention, mitigation of, and recovery from cyber incidents

Coordinate cyber threat investigations

Prosecute cybercrimes

DND

Lead for National Cyber Defense (AFPCYBERCOM)

Defend the military network from cyber attacks

Gather foreign cyber threat intelligence and determine attribution

Secure national security and military systems

Support the national protection, prevention, mitigation of, and recovery from cyber incidents

Investigate cybercrimes under military jurisdiction (cyberdefense)

INTELLIGENCE COMMUNITY:
CYBER THREAT INTELLIGENCE AND ATTRIBUTION

(NSC, NICA)

NATIONAL CYBERINTELLIGENCE PLATFORM:
SHARED SITUATIONAL AWARENESS

IDENTIFY PROTECT DETECT RESPOND RECOVER

COORDINATE WITH PUBLIC, PRIVATE AND INTERNATIONAL PARTNERS

ttin

A. Requirements in establishing a CERT

- Design your CERT Framework
- Know your Organizational Structures

ettin

A. Requirements in establishing a CERT

- Design your CERT Framework
- Know your Organizational Structures
- Strategy how you start it / Initial Policies / Phases

Cybersecurity STRATEGY

- Tools based
- Reactive / Manual

Cyber Resilient Philippines

How do we get there?

- Crafting of the National CyberSecurity Strategy, Policies, Plans and Programs
- Establishment of NCERT and Implementation of other Programs defined in the National Cybersecurity Plan

ettin

A. Requirements in establishing a CERT

- Design your CERT Framework
- Know your Organizational Structures
- Strategy how you start it / Initial Policies / Phases
- Mission / Objectives
- Funding
- CERT location
- Staff/Team skills
- Define Processes

B. Type of CERT

- National CERT

* act as the main national point of contact for domestic incident response stakeholders as well as other national CERT around the world

B. Type of CERT

- Sectoral CERT

* serve as incident response for specific sector of society such as banking, energy, healthcare etc.

B. Type of CERT

- Government CERT

* are tasked with monitoring and responding to incidents on internal networks of government agencies. All sub branches/locations are also covered.

B. Type of CERT

- Organizational CERT

* This can be individual organization or business for incident handling within the organization

C. What Type of services should be offered

Reactive Services

- Alerts and Warnings
- Incident Handling
- Incident Analysis
- Response Support
- Incident Response Coordination
- Incident Response on Site
- Vulnerability Handling

C. What Type of services should be offered

Reactive Services

- Vulnerability Analysis
- Vulnerability Response
- Vulnerability Response Coordination

C. What Type of services should be offered

Proactive Services
- Announcements
- Technology Watch
- Vulnerability Assessments
- Penetration Testing
- Configuration and Maintenance of Security Tools
- Intrusion Detection
- Security Services
- Information Dissemination

C. What Type of services should be offered

Artifact Handling

- Artifact Analysis
- Artifact Response
- Artifact Response Coordination

C. What Type of services should be offered

Security Quality Management

- Digital Forensics
- Risk analysis
- Business Continuity and Disaster Recovery
- Security Consulting
- Awareness Building
- Education/Training Product Evaluation or Certification

ttin

D. How big is the CERT?

- Existing IT Team
- Hire a complete CERT
- Outsource only / Managed Services

E. Incident Response Capability

- Structures
- Available Tools
- Management Systems

oles

Data/Information Handling

Determine who is allowed to use? Who will grant or approve access? What are the responsibilities of the following? Rights? (Head Systems Administrator, Team Lead, Analysts, other technical team, Vendor, Focal person)

- Sensitive Information
- Logs
- Information Flow
- Storage
- Damage Data

oles

Procedures

- General CERT flow
- Policy
- Security Checklist
- Contacts

ples

Recovery

- Disaster Recovery Policy

ples

Recovery

- Disaster Recovery Policy

according [illegible] 2021)

Technical Excellence:

The CERT should have the most up to date resources and advice and in order to maintain this advantage, the advice they give must be sound which requires high levels of technical excellence. This may lead to the CERT only being initially with a small number of good quality capabilities rather than lots of poor quality capabilities.

according 2021)

Trust :

If the organizations and end users do not explicitly trust the CERT then they will be unable to share data with the CERT and will not be able to use all the facilities on offer. The trust is crucial for partner organizations and the organizations themselves would want confirmation that the CERT can handle sensitive information responsibly.

according [illegible] 2021)

Resource Efficiency:

The CERT must be constantly adapting by analyzing potential new threats and their potential impact. This will then help to steer the allocation of funding sources to test, which treats and incidents are truly of interest to the CERT.

according [illegible] 011)

Cooperation:

The CERT should cooperate as fully as possible (taking into account the sensitivity of some of their clients’ data) with national stakeholders, government and other CERTs so that the knowledge can be shared and they can collaborate on complex problems.

QUESTIONS?

fb.com/cybersecgovph   fb.com/ciccgovph   fb.com/ncertgovph

QUESTIONS?

alwell.mulsid@dict.gov.ph

END OF PRESENTATION

DICT
DEPARTMENT OF INFORMATION AND COMMUNICATIONS TECHNOLOGY