FEMA Region III Cyber Security Program

Maryland Cyber Security Workshop (January 16, 2019)

(Presented again at the October 16, 2018, meeting of the Maryland Cybersecurity Council and published with permission.)

Overview

ƒ Current Landscape

ƒ Challenges

ƒ Review current resources (Federal and State)

ƒ Discuss information flow for reporting an incident

ƒ Discuss what prompts a report and determines who is called

ƒ)(0$¶V 5ROH LQ D &\EHU ,QFLGHQW DQG 5HJLRQ ,,,¶V ZRUN

Current Landscape

- &\EHUVHFXULW\ LV QRW ³VROYDEOH´
    - State and Territory Self-Reported Capability Levels - Cybersecurity is the lowest rated of the capabilities
- Progress has been made, but more needs to be done
    - Cybersecurity roles and responsibilities across the stakeholder community remain unclear
        - Feedback from State Partners ±who do we call for an incident? Which federal partner is the lead? How do we get better information? ±need DHS and FEMA HQ to continue these discussions
    - All-hazard doctrine has started to, but does not fully address the impacts of cybver events
    - Training and exercises will be required to continue to institutionalize cyber preparedness and response
    - Cross stakeholder coordination LV HVVHQWLDO DQG PXVW JURZ SDVW WKH ³JHW W

Challenges Surrounding Responding to Cyber Incidents

ƒ End User Error

ƒ No geographic boundary

ƒ Fast spreading

ƒ Often must do investigation, mitigation and response all at one time

Federal Resources: Asset Response

- DHS National Cybersecurity and Communications Integration Center (NCCIC)
  -

Federal Resources – Asset Response

ƒ DHS Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)

- Responds to and analyzing control systems-related incidents;
- Conducts vulnerability, malware, and digital media analysis;
- Provides onsite incident response services;
- Provides situational awareness in the form of actionable intelligence;
- Coordinates the responsible disclosure of vulnerabilities and associated mitigations; and
- Shares/Coordinates vulnerability information and threat analysis through information products and alerts.

Federal Resources: Asset Response

- USCG National Response Center

Federal Resources: Threat Response

ƒ United States Secret Service Field Offices and Electronic Crimes Task Forces

- Report cybercrime, including computer intrusions or attacks, transmission of malicious code, password trafficking, or theft of payment card or other financial payment information

ƒ United States Immigration and Customs Enforcement/Homeland Security Investigations (ICE/HSI)

- Report cyber-enabled crime, including: digital theft of intellectual property; illicit e-commerce (including hidden marketplaces); Internet-facilitated proliferation of arms and strategic technology;

Intelligence/Information Resources

ƒ FBI Infraguard

- InfraGuard is a partnership between the FBI and members of the private sector. Infraguard is dedicated to information sharing and relationship building across organizations including state and local law enforcement agencies. While it also has a physical security focus, the program started with a cybersecurity case in 1996. Its 85 chay5a9(i)8.9(l)9(d)9(i)9.1(n(08(ty)8(pri)4(v(n(08(t [(1-36.4(a)9e)9(s)-2

Intelligence/Information Resources

- National Governors Association
  - The DVVRFLDWLRQ¶V Resource Center for State Cybersecurity aims to provide governors with resources and tools for implementing effective policies and practices on the topic. Launched in 2012, the LQLWLDWLYH¶V SULPDU\ goal is for states to develop strategies for strengthening cybersecurity practices as the relate to IT networks, health care, education, public safety, energy transportation, critical infrastructure, economic development and the workforce.

- NIST Framework for Improving Critical Infrastructure Cybersecurity
  - The framework is a living document of best practices that uses can reference to establish a risk-based approach to improve cybersecurity. The latest draft was released in January 2017. It

Intelligence/Information Resources

ƒ National Guard Cyber Protection Teams

- Cyber Command Readiness Inspections
- Vulnerability Assessments
- Cyber opposing force support (threat emulation)
- Critical Infrastructure Assessment

ƒ DHS Cyber Security Advisors (CSA)

- Great resource for information/trends
- Region III CSA: Franco Cappa

State Resources – Reporting

ƒ DC Washington Regional Threat Analysis Center

ƒ Delaware Information and Analysis Center

ƒ Maryland Joint Operand 7d 6m/gt

Triggers to report a Cyber Incident

ƒ What triggers would occur to make you contact someone (state or federal for assistance)?

- Potential Guide from National Cyber Incident Response Plan:
- Level 0: Nuisance DoS or defacement (No event or incident anticipated. This includes routine watch and warning activities.)
- Level 1: Commit a financial crime (Unlikely to impact public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.)
- Level 2: Steal sensitive information (May impact public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.)
- Level 3: Corrupt or destroy data/Deny availability to a key system or service (Likely to result in a demonstrable impact to public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.)
- Level 4: Damage computer and networking hardware (Likely to result in a significant impact to public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.)
- Level 5: Cause physical consequence (Poses an imminent threat to the provision of wide-scale critical infrastructure services, national government security, or the lives of US citizens.)

)(0$¶V 5ROH LQ &\EHU ,QFLGHQWV

-)(0$¶V UROH LQ WKH IHGHUDO JRYHUQPHQW¶V UHVSRQVH WR DQ WKH 1DWLRQDO &\EHU ,QFLGHQW 5HVSRQVH 3ODQ 1&,53 ZKLFK 3URWHFWLRQ DQG 3URJUDPV 'LUHFWRUDWH 133' DQG)(0$¶V 1D with interagency partners

- Existing policies and coordinating structures can handle the vast majority of cyber incidents, however significant cyber incidents may require the establishment of a Cyber Unified Coordination Group (UCG)

- Depending on the response activities needed to support the incident, FEMA may activate certain ESFs. 7KH VLJQLILFDQW F\EHU LQFLGHQW UHVSRQVH PHFKDQLVPV RXW and Integration section will coordinate with the established ESFs

NCIRP and FEMA

‡) (0 $ ¶ V emergency management responsibilities:

‡ FEMA is the Lead Federal Agency for coordinating the response to physical impacts of a cyber incident.

Effects on COOP following a Cyber Incident

ƒIf the Nation faces a significant cyber incident today:

ƒ Offline systems leave an elevated national security risk and keep government services from reaching survivors

ƒ

FEMA Region III Cyber Security Workshops

- Region III has hosted 3 workshops to date:
  - August 17-18, 2016 Workshop and TTX in Philadelphia, PA
    - Panels from federal, state and private sector partners
    - Presentation on National Cyber Incident Response Plan
    - Tabletop Exercise on Cyber Incident
  - July 25, 2017 Workshop in Suffolk, VA
    - Panel from state partners
    - Presentations on VA National Guard Cyber Teams, VA Fusion Center, FEMA Region III Cyber 411 Resource Guide, National Cyber Incident Response Plan
  - July 18, 2018 Workshop in Annapolis, MD
    - Panels from federal and state partners
    - Presentations on TEEX resources and Cyber Attack Demo, RAND study on Cyber Plans
  - Looking to partner with Delaware to host our next workshop in the summer of 2019

FEMA