REGION 5 CYBER DAWN TABLETOP EXERCISE (TTX)

OCTOBER 30, 2018
WELCOME AND INTRODUCTIONS

• Opening Remarks
• Introductions
SCOPE

• This exercise is a facilitated, discussion-based exercise, planned for four-and-one-half hours, hosted by PCEM.

• The exercise will raise awareness of cyber risk management, cyber related planning, and other issues related to cyber incident prevention, protection, and response.
EXERCISE OBJECTIVES

• Increase cybersecurity awareness to senior officials of cyber risk management, cyber related planning, and other issues related to cyber incident prevention, protection, response, and recovery of critical systems.

• Assess cybersecurity integration into an organization’s all-hazards preparedness.

• Examine cybersecurity incident information sharing, escalation criteria, and related courses of action.

• Examine cybersecurity incident management structures.

• Review cyber resource request and management processes.

• Assess the integration of the Region 5 Cyber Resiliency Concept of Operations (CONOPS).
EXERCISE OVERVIEW

• Four+ hour, continuous, interactive exercise that will require schedule discipline.

• The TTX consists of:
  • Introductions and Current Threat Landscape Briefing
  • Five Phased Modules
  • Debrief and Evaluation

• Participant engagement encouraged

• Time awareness during questions, brief outs, etc.
<table>
<thead>
<tr>
<th>Activity</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Welcome, Introductions, and Guidelines</td>
<td>15 minutes</td>
</tr>
<tr>
<td>Cyber Threat Landscape Briefing</td>
<td>15 minutes</td>
</tr>
<tr>
<td>Phase One – Preparation</td>
<td>45 minutes</td>
</tr>
<tr>
<td>Phase Two – Detection</td>
<td>45 minutes</td>
</tr>
<tr>
<td>Phase Three – Escalation</td>
<td>45 minutes</td>
</tr>
<tr>
<td>Phase Four – Notification</td>
<td>45 minutes</td>
</tr>
<tr>
<td>Phase Five – Containment, Eradication, and Recovery</td>
<td>45 minutes</td>
</tr>
<tr>
<td>Hot Wash and Closing Comments</td>
<td>15 minutes</td>
</tr>
</tbody>
</table>
ASSUMPTION AND ARTIFICIALITIES

• This exercise will be conducted in a no-fault environment and will evaluate the existing plans, policies, and procedures as if players were responding to a real-world emergency.

• Earnest effort has been made to create a plausible and realistic scenario to evaluate and validate identified objectives.

• The exercise is not to be viewed as a test or inspections of individual performance.

• There is no hidden agenda and there are no trick questions.
GROUND RULES

1. Do NOT critique the scenario
   - Trying to find holes or inconsistencies in the scenario is counter-productive and disruptive; the scenario should stimulate discussion

2. Draw from your previous experience
   - As you participate, please utilize your knowledge of how the Whole Community works together in response and recovery situations

3. Do NOT assume information
   - If questions arise that are not answered by the provided material, please ask the facilitator

4. Participation is encouraged
   - Speak freely, respect others when they are speaking
   - Participate in your disaster role as if the event were occurring
   - Processes and decision making are more important than the details

5. The facilitator's job is to help you generate solutions

6. Scenario is generic and uses common departments
   - In the event your organization doesn’t have the specified department please substitute the department with one that you feel would benefit from the exercise
Understanding the Current Cyber Risk

Presented by
Hillman Mitchell
Critical Infrastructure Cyber Security Consultants
THREAT ACTORS

• Criminals
• Hacktivist
• Insiders
• Nation States
THREAT LANDSCAPE – TOP THREATS

- Phishing
- Ransomware
- DDoS
- APT

Source SANS Institute
THREAT LANDSCAPE – TOP VECTORS
2017

- Email Attachment/Link
- Drive-by or download
- Web Server/Web App
- USB Drives

Source SANS Institute
THREAT LANDSCAPE – TIME TO DISCOVER & REMEDIATE
UPDATE 2018

• Adversaries malware high sophistication and impact
• Adversaries becoming more adept at evasion
• Adversaries weaponizing cloud services and legitimate technology
• Adversaries exploiting undefended gaps in security, Internet of Things (IoT) and use of cloud services
TRENDS

- Botnets continue to impact, infecting them with old/new malware
- Hackers went for the easy marks
- Low-cost attack methods with potentially high returns
- Ransomware appears to not be slowing down any time soon
DEFENDERS SHOULD CONSIDER

• Implementing first-line-of-defense tools that can scale, like cloud security platforms

• Adhere to policies and practices for patching
  • applications
  • systems
  • appliances

• Employing network segmentation to help reduce outbreak exposures
DEFENDERS SHOULD CONSIDER

• Patching
• Monitoring
• Detection
• Info Sharing (right not first)
DEFENDERS SHOULD CONSIDER

• Info Sec integrated
  • Design
  • Supply Chain
  • Operational Business/IT

• Info sharing -
  • Best practices
  • CTI

• Mutual Aid for Response & Recovery
THE VALUE OF TRAINING AND EXERCISING

• Identify gaps and potential improvements
• Builds “muscle memory”
• Builds Community
• Builds Resiliency
PHASE 1 - PREPARATION

Become the Cyber Warrior Every Organization Needs
11:00 a.m. — A City of Lakewood Public Works employee reports to the information technology department (IT) that he received an email from Finance directing all employees to update their timesheets in the Employee Timesheet System (ETS). The employee clicked a link in the email that opened what looked like ETS. However, after entering the user credentials, the employee received an unfamiliar error page.
INCIDENT DISCUSSION QUESTIONS

1. Do employees know what constitutes suspicious cybersecurity activities or incidents?
   a) Do they know what actions to take when one arises?
   b) What established processes exist for employees to report cybersecurity incidents?

2. Would any additional reports or notifications be made? If so, are designated points of contact identified?

3. What incident severity level or tier is a suspicious email?
ADDITIONAL QUESTIONS

1. What training do you provide in support of your cybersecurity incident response plan, business continuity plan, disaster recovery plan, emergency operations plan cyber incident annex, or other related plans?

2. Does your organization provide basic cybersecurity and/or IT security awareness training to all IT users (including managers and senior executives)?
   a) How often is training provided?
   b) Does it cover:
      i. General jurisdiction, department, and/or agency policy review,
      ii. Roles and responsibilities,
      iii. Password procedures, and
      iv. Whom to contact and how to report suspected or suspicious activities?
3. What security-related training does your organization provide to, or contractually require of:
   a) IT managers
   b) system and network administrators
   c) vendors
   d) other IT personnel having access to system-level software

4. Discuss your organization’s intrusion detection capabilities and analytics that alert you to a cyber incident.
PHASE 2 - DETECTION
3:00 p.m. — The City of Lakewood Service Desk receives five reports of emails similar to the one reported by the Public Works employee. Further investigation reveals that spearphishing emails were sent to employees across all Lakewood departments over a two-day period. The emails directed users to a spoofed website designed to capture ETS user credentials.
INCIDENT QUESTIONS

1. What is the incident severity level or tier of this incident once multiple spoofed emails are reported? What would prompt a change in tiers?

2. What immediate remediation and protective actions would be taken at your agency?
   a. Who is responsible for those actions?
   b. Have these options been documented in plans?
   c. How are they activated?

3. Would any additional reports or notifications be made? If so, are the primary, secondary, and tertiary points of contact identified?
1. What are the requirements and/or processes to notify agency leadership of a cyber incident at each severity tier?

2. Are these criteria the same across the enterprise, or do they differ by agency?

3. What resources and capabilities are available to analyze the intrusions:
   a) Internally?
   b) Externally through government partners?
   c) Through the private sector?
1. Discuss the role of cybersecurity in contracts with third-party support vendors and crucial suppliers. Have you discussed these types of concerns and risks with them?

2. What mechanisms and products are used to share cyber threat information within your organization and external to your organization (e.g., distribution lists, information sharing portals)?
PHASE 3 – ESCALATION
PHASE 3 - DAY 3: ZOMBIE ATTACK

10:00 a.m. — Pierce County Road Maintenance & Operations WebEOC - Active Response Board updates with a new incident for a five-car motor vehicle accident on Canyon Rd & 112th St E.

10:04 a.m. — WebEOC shows a posting for a wildfire near Canyon Rd & 112th St E.

10:10 a.m. — EOC staff confirm the motor vehicle accidents and wildfire postings are fake.

1:00 p.m. — WebEOC updates with a new posting for a “zombie attack” on Pacific Ave S & 152nd St E. EOC personnel work quickly to have erroneous postings pulled.
INCIDENT QUESTIONS

1. What immediate remediation actions would be taken?
   a) Who is responsible for those actions?

2. Are redundant systems in place if the impacted system(s) is compromised?

3. What is the incident severity tier of this event?
1. Do you have defined cybersecurity incident escalation criteria, notifications, activations, and/or courses of action?
   
a) If so, what actions would be taken at this point? By who?
   
b) Who would this incident be reported to?
   
c) Would any additional reports or notifications be made (e.g., to law enforcement for reasons related to public safety)? Are points of contact identified?
   
d) Would leadership be notified?
   
e) Does the organization report cybersecurity incidents to outside organizations? If so, to whom?
   
f) What, if any, mandatory reporting requirements do you have?

2. Are these criteria the same across the enterprise, or do they differ by agency?
ADDITIONAL QUESTIONS

1. How is information shared among your internal and external stakeholders—through formal or informal relationships? What information sharing mechanisms are in place?

2. Do you have processes to ensure that your external dependencies (contractors, power, water, etc.) are integrated into your security and continuity planning and programs?
PHASE 4 - NOTIFICATION

CYBER ATTACKS AHEAD

WHO YA GONNA CALL?
PHASE 4 - DAY 4: MESSAGE RECEIVED

12:00 p.m. — Multiple information sharing partners contact the South Sound Regional Intelligence Group (SSRIG) regarding a hacker advertising City of Puyallup cyber vulnerabilities, inciting their exploit, and selling Puyallup tax records.

The reports show that at 2:30 a.m. on Day 2, user “B1gM0n3y” posted a message in a known hacker forum alerting readers that the Puyallup government has Windows XP vulnerabilities that can be easily exploited. The user boasted that he accessed tax records from the Finance Department and is selling citizens’ personally identifiable information. To prove these claims, “B1gM0n3y” posted a screenshot of the tax data.
INCIDENT QUESTIONS

1. From which information sharing partners would you expect to receive this information (e.g., FBI, USSS, MS-ISAC, US-CERT)?

2. Which department/organization would receive the information?

3. How and to whom would the department/organization further disseminate this information?

4. Are there flowcharts showing the high-level relationships and crisis lines of communication (i.e., who calls who) specifically for a cyber incident? Are they part of the response or continuity planning documents?

5. What are your essential elements of information and key information questions necessary for operational and executive-level responses to cyber incidents? Where are they documented?
1. What immediate protection and mitigation actions would be taken? Who is responsible for those actions?

2. What, if any, mandatory reporting requirements do you have? Are additional reporting requirements in place for the loss of personally identifiable information (PII)?

3. At what point in the scenario would you contact law enforcement and/or the state Attorney General?
   a. How would relationships with law enforcement and other partners be managed? Where is the process documented?
   b. How does a law enforcement investigation impact containment, eradication, and recovery efforts?
   c. Are processes and resources in place for evidence preservation and collection?
   d. What are your expectations of state and federal government?
ADDITIONAL QUESTIONS

1. Compare and contrast incident management when incident detection occurs internally and when incident detection originates from external stakeholders notifying your organization.

2. What cyber related public information planning has occurred?
   
a. Who is responsible for public information related to the incident?

b. Have public information officers and other spokespersons been trained on cyber specific terminology or otherwise been prepared for a cyber incident?
PHASE 5 – CONTAINMENT, ERADICATION, & RECOVERY
PHASE 5 - DAY 5: ON THE DEFENSIVE

• **9:00 a.m.** — After being alerted that hackers are targeting government agencies, the Tacoma-Pierce County Health Department (TPCHD) reviews its logs and finds a large amount of data has been exfiltrated from the TPCHD systems in the previous 48 hours. Bates Technical College performs a similar review and finds a similar data breach. The Pierce County Sheriff’s Department (PCSD) reviews its logs and finds a rogue device on the network. Other agencies have not found evidence of any breaches at this time.

• **8:00 p.m.** — PCSD officials recovered the rogue device—an unauthorized laptop—and discovered Supervisory Control and Data Acquisition (SCADA) malware files stored on the computer. The initial analysis of the malware indicates the malware allows for control of jail cell doors.
INCIDENT QUESTIONS

1. Who would these incidents be reported to?

2. What, if any, additional notifications or actions would this prompt?
   a. Are points of contact identified?
   b. Are additional reporting requirements in place for the loss of protected health information (PHI)?

3. Collectively, would these events be considered the highest level of incident severity?

4. What immediate protection and mitigation actions would be taken at your agency?
1. What would the incident management structure look like? Who is assigned to key positions?

2. What resources and capabilities are required to respond to the incidents?
   a. Are these available within Pierce County?
   b. Are processes in place to request external resources or capabilities if needed?

3. Would these events trigger activation of the Region 5 Cyber Resiliency Concept of Operations? If so, would that alter any department roles and responsibilities?
1. Would these events and the events of the previous five days be jointly managed?

2. Who declares the incident is over? What are the criteria for declaring the response complete?

3. Describe your role in post-incident activity.

4. What is your role in restoring and/or maintaining public confidence?

5. Have your information security officers and emergency managers jointly planned for cybersecurity incidents?

6. Are IT and business continuity functions coordinated with physical security? Are all three then collaborating with public relations, human resources, and legal departments?
CLOSING COMMENTS

• Thank you for participating

• Please do not forget to complete the Participant Survey Form and return it to the Exercise Facilitator

• Conduct Exercise Hot Wash now
QUESTIONS?

Natalie Stice, AEM
Homeland Security Coordinator
Pierce County Emergency Management
natalie.stice@piercecountywa.gov
(253) 798-3311

DHS National Cyber Exercise and Planning Program (NCEPP)
cep@hq.dhs.gov
(703) 235-5641