



Homeland
Security

Cyber Intrusions: More than an IT Challenge

ICSJWG Fall Meeting

October 16, 2012

Presented by: Bridgette Walsh
DHS Cyber Exercise Program (CEP)

State of the World: Cyber Realities

- Increasing frequency, scope, and complexity of cyber attacks against the private/public sectors.
- Underscores need for a more robust organizational cyber incident response capability.
- “All-hazards” integration - Where does cyber fit in?
 - Presents unique challenges due to diverse attack vectors, widespread impacts, and complex mitigation.



Underlying Challenges

- How can an organization effectively balance traditional incident response needs with those necessitated by a cyber intrusion?
- How can an organization ensure a robust cyber incident response capability when faced with limited security resources?



Good IT is a given

- IT staff are key to effective cyber response:
 - Play mission-critical role in cyber incident response
 - Traditional “first responders” to a cyber breach
 - Possess the technical “know-how” to respond to and contain the immediate impacts of a breach
- However, good IT is only one piece of the response puzzle.

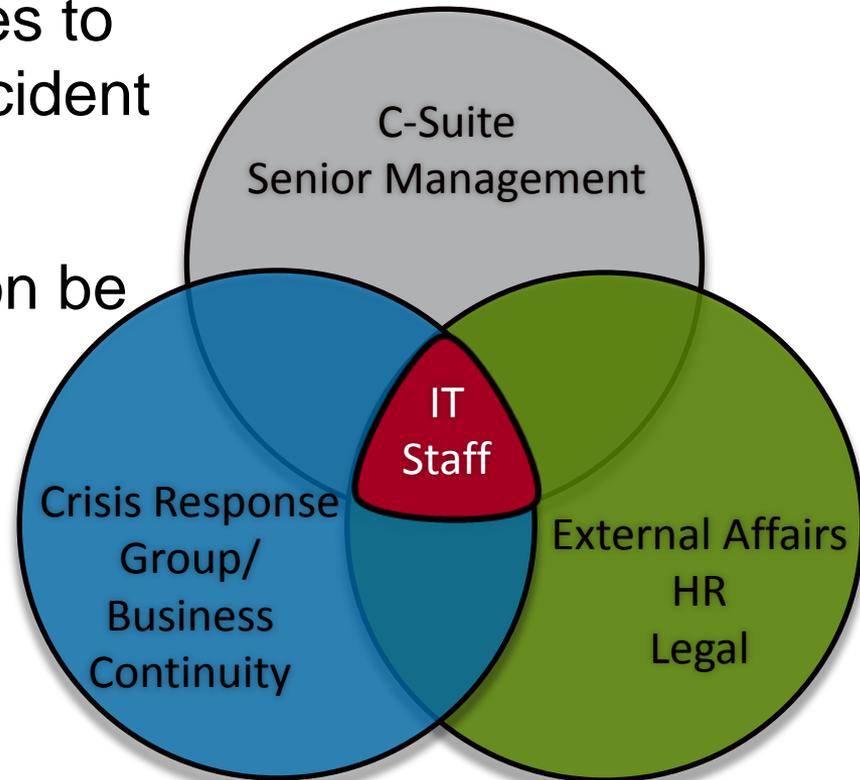


The IT Communications Gap

- IT management alone of a cyber incident is not the key to an effective “whole organization” response – must have robust communications across the organization:
 - Example: Sony PlayStation3 breach – took 6 days to warn customers of “potential” breach of personal information/credit card data
 - Told customers passwords were stored in database as *unencrypted* and did not fully explain (until much later) that stolen passwords were hashed – could IT, external affairs, and the rest of the organization have communicated more effectively with one another?

Cyber Incident Management Team

- IT staff must work closely with other key organizational entities to guide/inform effective incident response.
- How can this coordination be defined, practiced, and formalized?

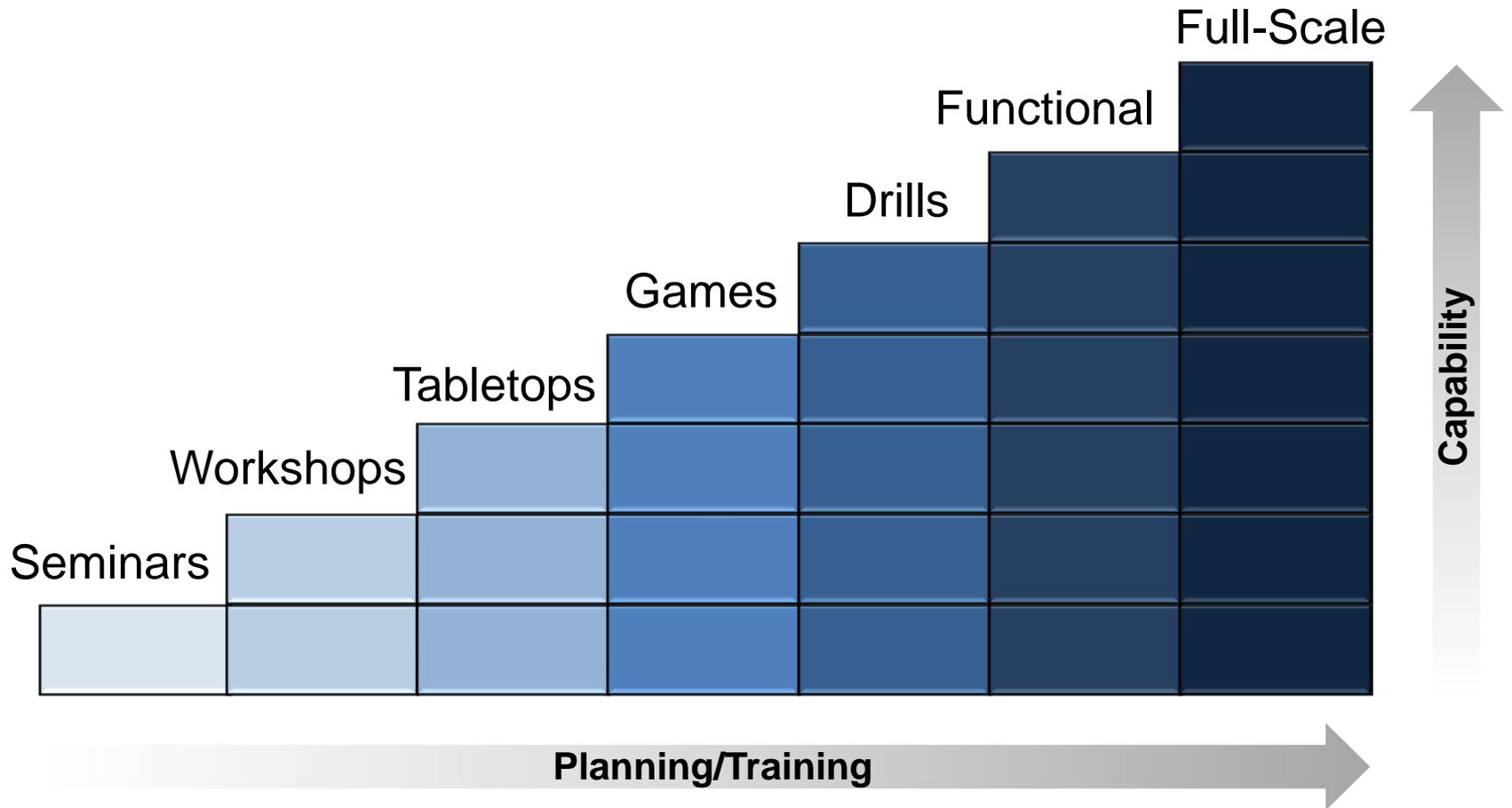


Cyber Exercises: A Proven Tool

- Cyber exercises help organizations:
 - Prepare for current threats, emerging vulnerabilities, and direct/indirect impacts associated with a cyber attack
 - Reveal organizational, policy, and operational gaps/overlaps
 - Encourage joint action and collaboration across a wide range of internal and external stakeholders
- Not a question of “if” but “when” – practice how you fight!



Cyber Exercises: Types



Do we exercise? If so, how?

- Most organizations do conduct cyber exercises, but what types?
 - Technical in nature – solving an IT problem
 - Contain the breach; analyze the malware; perform forensics – reinforce training
 - Test defined response plans/protocols/procedures
 - Business Continuity Plans; Crisis Response Frameworks – function/division specific
- Good, but these “exercises of validation” are not all-encompassing.





Essential Tool: “Exercises of Discovery”

- Exercises of “discovery”:
 - Seek to involve the broader response elements of an organization
 - Address not only the technical mitigation of a cyber attack but also key internal and external communications processes
 - Forge response relationships, communications channels, and help define response roles
 - Identify capability gaps and areas for improvement
 - Inform strategic planning and security investment



So what are we discovering?

What are the main organizational trends that we see revealed through cyber exercises ?

Trend 1: Cyber Information Sharing

- IT should be the primary clearinghouse for cyber threat, vulnerability, and incident information.
- However, information received by IT is not always shared with the broader response elements of an organization
- IT staff must be able to effectively communicate:
 - Cyber risk – realized/potential impacts
 - Recommended courses of action
 - To senior leaders, external affairs, legal, etc.
– all in **understandable terms**





Trend 2: Command and Control (CC)

- Organizations typically implement adequate CC mechanisms for *internal* cyber incidents.
- However, when involving external entities in cyber incident response – e.g., law enforcement, state/government agencies, other sector partners/third-party security vendors:
 - CC can often become overly complex and lack clear definition.
- Organizations must strive to clearly define incident command roles and responsibilities associated with small, medium, and large-scale cyber attacks.

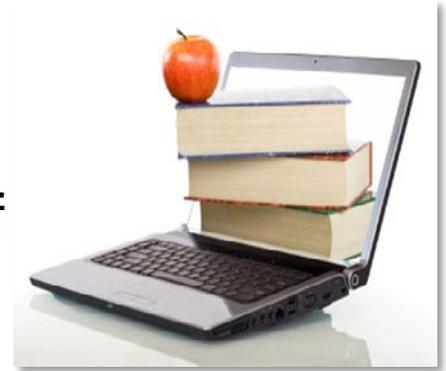


Trend 3: Internal/External Comms

- IT and continuity often do not collaborate closely with one another on a regular basis – resulting in an uninformed perception of the other’s roles/available resources that can be leveraged during a cyber incident.
- IT and external affairs must communicate effectively during a cyber incident – these channels ensure customer messaging is timely, accurate, and intelligible.
- IT and legal department must communicate effectively regarding any legal implications/restrictions involved in cyber incident response.

Trend 4: Cyber Training and Education

- Biggest challenge orgs face: lack of user awareness and cyber-ed.
- While many orgs do conduct some form of cyber awareness training for employees, this training is often:
 - Infrequent (i.e., only for “new-hires” or on an ad-hoc basis)
 - Lacking in current/relevant material
 - Non-mandatory – resulting in poor user retention or general lack of awareness among employees.
- One solution: Involve employees in a cyber exercise!





How do I plan a cyber exercise?

What are the main considerations for planning a cyber exercise at my organization?

Cyber Exercises: Planning Considerations

- Planning requirements depend on exercise type, scope, and determined objectives.
 - At the organizational level, successful planning typically requires several weeks to months
- Organizations should form an exercise design team:
 - Comprised of key incident response elements (e.g., IT, legal, HR, external affairs, crisis management, senior leadership)
 - Meet regularly to develop and reach consensus on exercise goals and objectives, exercise scenario, participants, and exercise logistics

Cyber Exercise: Scenario Development

- Scenarios should be realistic, grounded in exercise objectives, and should drive exercise discussion/action among *all* players.
- Orgs need *not* spend an exorbitant amount of money to make an exercise interactive, “entertaining”, or highly-operational.
- A successful exercise often involves a half or full-day, facilitated “tabletop” discussion among a diverse group of key organizational players.



Cyber Exercises: Common Challenges

- Resource Constraints...
 - Effective cyber exercises can be done with little or no cost to an organization
- Senior Leader Buy-In...
 - Unfortunately, cyber threats are often not given due consideration until a significant incident occurs
 - Design the exercise to serve as the guiding component of an organization's regular business impact/risk analysis process

Cyber Exercises: Common Challenges

- Lack of Exercise Subject-Matter Expertise...
 - Not rocket-science/Call CEP!
- Nobody is available to participate?
 - If senior leaders buy-in so will others
- “We never learn anything from exercises...”
 - Then you are not conducting the right type of exercise. Exercises should be challenging, thought-provoking, even uncomfortable at times.

Building a Culture of Exercising: CTEP

- Organizations should establish a Comprehensive Training and Exercise Program (CTEP) to ensure cyber exercises continue on a regular basis, key outcomes are documented, and improvements are made.
- CTEP has four distinct phases:
 - Plan
 - Train
 - Exercise
 - Improve
- It's a continuous process!





How can CEP Help?

- CEP works closely with Federal, state, local, international, and private sector stakeholders to provide:
 - Design, execution, and evaluation support for both discussion-based and operations-based cyber exercises
 - Exercise planning and facilitation, scenario and injects development, after-action analysis, and overall cyber exercise design consultation
 - LLIS.gov CEP page – wealth of cyber exercise resources
 - CEP *Cyber Scenario Sampler and SitMan Library*
 - Critical Infrastructure TTX in a Box (Chemical, Health, Critical Manufacturing so far)
 - *Joint CSEP TTX in a Box – Post CSEP Assessment* *



Conclusion/Wrap-Up

Questions?



DHS Cyber Exercise Points of Contact

Bridgette Walsh

Deputy Director, CEP
National Cyber Security Division
bridgette.walsh@dhs.gov
703-235-2887

Cyber Exercise Program

National Cyber Security Division
CEP@DHS.gov



**Homeland
Security**