National Level Exercise 2012: Cyber Security Table Top Exercise

Facilitator Background Information

A Tabletop Exercise (TTX) is a discussion-based exercise, with a facilitated discussion of a scripted scenario in an informal, stress-free environment. It is designed to elicit constructive discussion as participants examine and resolve problems based on existing operational plans and identify where those plans need to be refined.

The scenario of this TTX will reference websites, adversaries, companies and subject matter experts that are fictional and are not intended to replicate or represent a particular entity or person.

As facilitator, your role is to create a framework that encourages dialogue and guide discussions to meet the objectives of this exercise, capture innovative ideas, create teamwork, and educate participants. Within this document we've provided suggested language for each slide that will engage exercise participants effectively and appropriately. Additionally, we recommend including the most appropriate people within your company or organization to participate in this exercise in order to have the most beneficial experience and outcomes.

Please note that the time needed to conduct this exercise is flexible. It is estimated that it will take anywhere from two to four hours total. Because cyber security is such a broad topic area, we recommend that exercise FACILITATORS review this presentation thoroughly and customize it to their organization's needs before use. To aid FACILITATORS in doing this, on the discussion slides, we have color-coded the suggested questions as follows:

- *The ten questions labeled **PARTICIPANT** are the ones where FEMA would like participants' input, feedback and ideas. If your group desires to do this, following the exercise we invite you to share with us at **www.fema.gov/plan/nle**.*
- *The questions labeled **DISCUSSION** are intended to facilitate discussion around key topics, and are recommended for use by all.*
- *The questions labeled **ALTERNATE** are alternate questions that can be customized to drill down into key topic areas as desired.*

Slide 1 - Cyber Capabilities: [TIMING OF SLIDE: 2 minutes]

FACILITATOR: Welcome, everyone! My name is [INSERT NAME], and I will be leading you through today's Tabletop Exercise on cyber capabilities. This exercise was developed by the Federal Emergency Management Agency for use by private sector preparedness partners as a part of National Level Exercise 2012. The exercise is designed to help us evaluate our emergency response plans, processes and procedures and identify any gaps or shortfalls that we can strengthen in the future.

As we go through today's exercise, you'll notice that the scenario and situations we encounter are pretty serious. The exercise has only been designed this way to expose you to the reality of a situation like this, NOT to intimidate you – there are no wrong answers here.

Housekeeping *[NOTE - Customize these to your organization's operations and policies]*: The exercise may take us up to four hours to complete. We will take two 15 minute breaks during the exercise. Please quiet your mobile phones and only use them in an emergency. Note that restrooms are located [WHERE], and emergency exits are located [INSERT LOCATION].

Slide 2 - Agenda Review: [TIMING OF SLIDE: 5 minutes]

FACILITATOR: Before I walk you through the agenda, let's all introduce ourselves.

[Participants introduce themselves]

FACILITATOR: Thank you. As we get started, I'd like to call your attention to our agenda.

We will start with a general overview during which I will share details on National Level Exercise 2012 (which this TTX is a part of), today's goals, ground rules and information on how exactly we will benefit from participating in this TTX.

After walking through the overview, we'll move through three modules of the exercise that will take us through an evolving cyber event – covering the initial threat alert, a sustained and comprehensive attack, and the aftermath of an attack. Each module is designed to facilitate discussion and thought generation around our capabilities in responding to and recovering from these very specific situations.

After we've gone through each module, we'll discuss our key outcomes and/or results and, if we choose, share them with FEMA and its NLE 2012 partners. By doing this, we can amplify the impact of our exercise today and help shape future decision-making throughout the entire emergency management community.

Slide 3 - Exercise Overview: [TIMING OF SLIDE: 5 minutes]

FACILITATOR: First things first. What is a National Level Exercise and why does it matter to us?

Part of the NEP

For those of you who are unfamiliar with the term, a National Level Exercise (or NLE) is a large-scale, multi-jurisdictional exercise that occurs annually as part of the National Exercise Program (or NEP), which is a congressionally-mandated preparedness series that focuses on potential catastrophic events. All levels of government and a wide range of private sector partners participate in NLE 2012.

The NEP serves as a means to exercise national preparedness, validate plans, test operational capabilities, maintain leadership effectiveness and examine the ways we work with the entire community to prevent, protect from, respond to, recover from, and mitigate disasters and acts of terrorism.

Whole Community Focus

FEMA is currently leading the adoption of the “whole community” approach – which recognizes that every individual and every organization has an important role in making our communities, and the nation as a whole, more resilient – throughout the emergency management community.

NLE 2012 is a big part of this – unique to this exercise will be an emphasis on the shared responsibility among all levels of government, the private sector and the international community to respond to a catastrophic event.

Cyber Event Scenario

The NLE 2012 scenario focuses on the nation’s ability to coordinate and implement prevention, preparedness, response and recovery plans and capabilities pertaining to a significant cyber event or a series of events. In addition, the process examines national response plans and procedures, including the National Cyber Incident Response Plan, National Response Framework (or NRF), NRF Cyber Incident Annex, and more.

Slide 4 - Exercise Overview: [TIMING OF SLIDE: 3 minutes]

NLE 2012 Goals

FACILITATOR: The overall goals of NLE 2012 are:

- To examine information sharing among public-private partners and the overall general public;
- To assess decision making during a significant cyber event; and
- To evaluate government roles and responsibilities during a significant cyber event.

Benefits of Whole Community Participation

As you would imagine, participating in NLE 2012 offers many benefits to whole community organizations – including us! Participation in NLE 2012 allows us to contribute to:

- The achievement of a better collective understanding of the cyber threat within and across sectors;
- Increased understanding and greater evaluation of cyber threat alerts, warning, and information sharing across sectors and between government and the private sector;
- Increased understanding of government and private sector roles and responsibilities in cyber event response and recovery; and
- The testing and evaluation of government-private sector coordinating structures, processes, and capabilities regarding cyber event response and recovery.

Again, at the end of today's session, we will have the opportunity to share our ideas and outcomes with FEMA and others involved with NLE 2012. I am happy to do this for the group, or you can individually do so at **www.fema.gov/plan/nle**.

Slide 5 - Exercise Overview: [TIMING OF SLIDE: 3 minutes]

Exercise Ground Rules

FACILITATOR: To ensure today's conversation is as productive as possible, there are a few ground rules that you should keep in mind. The effectiveness of a tabletop exercise comes from the energetic involvement of participants, so these rules are designed to stimulate discussion that's both creative and structured. So as you participate in this exercise, please keep in mind the following:

- There are no right or wrong answers. All ideas are welcome and will be captured and acted on as appropriate.
- Maintain a no-fault, stress-free environment. It's very important that today's discussion is driven by group decision making and problem-solving, so the environment in this room must remain open, positive and encouraging.
- Use the scenario to provide context and spark creative ideas. All ideas and thoughts should be based on the information provided by the scenario, but this should not limit your thinking.
- Do not limit the discussion to official positions or policies. Don't be afraid to go beyond your title/position as you think about the situations that are presented.
- Tap community resources and assets to aid and enhance your brainstorming. Go beyond this organization's four walls to consider how you can be aided by and provide aid to your community during a disaster. In other words, maintain a whole community mindset!

We're now about to start the exercise. Before we move into the first module, are there any questions on the information we have reviewed so far?

[RESPOND TO QUESTIONS]

Slide 6 - Module #1: [TIMING OF SLIDE: 2 minutes]

FACILITATOR: We've now come to the first module, which focuses on introducing the cyber event scenario and discussing the ways in which we can increase our preparedness for a potential cyber threat. For the duration of the exercise, our simulated company will be known as Worldwide Global, Inc. This will help us to truly insert ourselves into the scenario, and ensure we fully grasp what unfolds during the exercise.

Coming up, you’ll receive information from Virtual News Network (or VNN) anchor Jeanne Meserve who will explain the current situation and provide key details that will be important to the discussion that follows and the rest of the exercise. We’ll also receive information from a third party with very specific experience in cyber attacks.

Just to give a little bit of background on the terms “hacker” and “hacktivist”, the two terms refer to a person (a hacker) who exploits software vulnerabilities to take control of computer systems, force the system to execute malicious code, or crash the system to deny its usage to a legitimate user. Hacktivists tend to be a group of hackers who exploit software vulnerabilities for a political gain.

Additionally, the term ’zero day’ exploit, as defined by the United States Computer Emergency Readiness Team (US-CERT), is “one that takes advantage of a security vulnerability previously unknown to the general public.” An attacker using a ‘zero day’ exploit is a severe threat as not even the software developer is aware of the vulnerability yet and has not issued a patch to fix the problem.

Slide 7 - VNN Inject #1 – [TIMING OF VIDEO: 5 minutes]

Please see VNN inject #1 script for details.

Slide 8 - Discussion 1 – Preventative Measures [TIMING OF SLIDE: 25 minutes]

[FACILITATOR LEADS discussion. In addition to these questions, FACILITATOR can prompt the participants with more specific questions customized to the organization/community.]

FACILITATOR: Now that we just received that information from VNN, let’s discuss our initial thoughts and address some initial questions. We just heard the report on planned hacktivist actions against U.S. interests, and the report was confirmed by various cyber security firms.

PARTICIPANT : At this point, the most important question for us to address is, do we feel compelled to take any preventative measures?

We are going to do just that, in groups, in just a moment. In addition to that main question, please also consider and address the following:

- ***DISCUSSION***: How do variables in the threat information that we receive – such as timeframe, credibility, and specificity – impact our decision making and prevention efforts?
    - ***ALTERNATE:*** In your opinion, what defines the difference between a hacker and hacktivists? Does this difference influence your decisions to take preventative actions?
    - ***ALTERNATE:*** If the hacker were a part of a criminal organization, would that influence your actions? How you respond?

- ***DISCUSSION***: What tools do we use to support cyber prevention? Are they sufficient?
  - ***ALTERNATE:*** How do we share cyber threat information internally? What about externally, with groups like law enforcement entities?
- ***DISCUSSION:*** What are our expectations of the federal government for cyber preparedness planning products or efforts? Do we coordinate with them? Should we?

[FACILITATOR instructs each table of participants to discuss each question among themselves.]

[AFTER 10 MINUTES, FACILITATOR asks a representative from each table to stand and share ONE OR TWO MAJOR AREAS OF AGREEMENT /COORDINATION, AND ONE OR TWO MAJOR AREAS OF DISAGREEMENT/CONFUSION. These are discussed with all the participants in the room and captured on paper, laptop or other media for later follow up.]

FACILITATOR: Now that we've shared our initial thoughts and discussed initial questions, let's talk about a few things that the news didn't report on.

Slide 9 - Internal IT Security Issues [TIMING OF SLIDE: 5 minutes]

FACILITATOR: What VNN didn't tell you was that, at the same time that this news was breaking, a minor IT security issue developed here at Worldwide Global, Inc. – which, remember, is <u>us</u>. It started when, driven by the discovery of a virus on an employee's computer, an IT manager conducted an enterprise-wide IT security audit.

What the IT manager found was significant enough to cause our company, Worldwide Global, Inc., to revise its IT access control and general computer use policies. Now managers are required to review the access permissions of all employees and abide by the concept of "least privilege," where a user should be given only those privileges needed to complete their assigned tasks.

Through the audit, IT security also identifies an active account for an employee who was terminated last month for repeatedly bypassing controls and accessing restricted information on the network. This discovery means that he could still have access remotely with this account. As a protection and prevention measure, IT security disables the account immediately and a review of the user logs find no activity following the employee's final day of employment.

As we move to the discussion part of this inject, focus on the impact that these two developments – the hacktivists and these internal issues – would have on our actions at this point.

Are there any questions before we begin brainstorming and discussion?

[RESPOND TO QUESTIONS]

Slide 10 - Discussion 2 – Planning and Policy [TIMING OF SLIDE: 25 minutes]

[FACILITATOR LEADS discussion. In addition to these questions, FACILITATOR can prompt the participants with more specific questions customized to the organization/community.]

FACILITATOR: At this point, we know that hacktivist organizations are threatening U.S. interests, and we're experiencing some abnormalities in our own system. Let's step back and focus on two very important questions:

- ***PARTICIPANT***: How do we currently integrate cyber preparedness into our emergency planning efforts? Are there ways that this can be improved?
- ***PARTICIPANT***: What policies and procedures do we have in place to ensure adequate cyber preparedness? Are these policies adequate, do we need to change any of them?

As you discuss these questions in your groups, you may also address the following related questions:

- ***DISCUSSION:*** How well does our organization currently integrate cyber security into the life cycle system (i.e., design, procurement, installation, operation and disposal)?
    - ***DISCUSSION:*** Are audits conducted on our cyber security systems? Are the systems compliant to our company's security plan requirements?
    - ***ALTERNATE:*** Do we ensure that service providers (i.e., vendors) that have access to our systems are following appropriate personnel security procedures and/or practices?
    - ***ALTERNATE:*** Discuss the decision making involved when determining internet access required for business versus restrictions that support cyber security.
    - ***ALTERNATE:*** Does our organization have an asset inventory of all critical IT systems and a cohesive set of network/system architecture diagrams or other documentation (e.g. nodes, interfaces, and information flows)?
- ***DISCUSSION:*** Who are our cyber preparedness stakeholders (public, private, non-profit, other)? Why are they important?
    - ***ALTERNATE:*** Do we have established cyber security risk-based performance standards?
    - ***ALTERNATE:*** Where do we receive our cyber planning technical assistance?
- ***DISCUSSION:*** What are our policies and procedures upon being notified of a compromise/breach of security regarding an employee?
    - ***ALTERNATE:*** Who is notified and what steps are followed to ensure this individual's access to facility and/or equipment has been terminated? What steps are followed from beginning to end?

        - ***ALTERNATE:*** Should legal representation be sought and at what point? Who determines if the employee should be held criminally responsible?

- ***DISCUSSION:*** Do we have a formal or informal policy or procedures pertaining to IT account management?

    - ***ALTERNATE:*** Do these policies or procedures include protocols for establishing, activating, modifying, disabling, and removing accounts?

    - ***ALTERNATE:*** Do these policies or procedures include protocols/steps for notifying IT account managers/administrators when users are terminated?

    - ***ALTERNATE:*** Does our organization eliminate information system access upon termination of an individual's employment?

- ***DISCUSSION:*** Do we employ a formal sanctions process for personnel failing to comply with information security policies and procedures? If so, has this been communicated to employees and how often?

[FACILITATOR instructs each table of participants to discuss each question among themselves.]

[AFTER 10 MINUTES, FACILITATOR asks a representative from each table to stand and share ONE OR TWO MAJOR AREAS OF AGREEMENT /COORDINATION, AND ONE OR TWO MAJOR AREAS OF DISAGREEMENT/CONFUSION. These are discussed with all the participants in the room and captured on paper, laptop or other media for later follow up.]

Slide 11 - Break: [TIMING OF SLIDE: 15 minutes]

FACILITATOR: Thank you everyone. At this time we're going to take a fifteen minute break, during which time I'll be looking to capture our best thoughts. If you have any additional feedback for this module that you'd like to share, feel free to let me know during this time. You can also use this time to grab a quick refreshment or restroom break if you need to, keeping in mind that we'll have another break later on.

Slide 12 - Module #2: [TIMING OF SLIDE: 1 minute]

FACILITATOR: We've now reached the second module. As we watch the following VNN reports, you'll see that the hacktivists are acting on their threats – and their target is Worldwide Global, Inc.! From fake invoices to extortion threats, it seems that The Void has managed to work its way deep into our networks.

As you watch, pay attention to The Void's tactics and their effects on our company, our customers and our stakeholders. Think about all of the steps that we'd be taking as we tried to respond to and stop the attack.

Slide 13 - VNN Inject #2: [TIMING OF VIDEO: 5 minutes total – segments are presented in short bursts]

Please see VNN Inject Script #2 for details.

Slide 14 - Discussion 1 – Detection and Response [TIMING OF SLIDE: 25 minutes]

[FACILITATOR LEADS discussion. In addition to these questions, FACILITATOR can prompt the participants with more specific questions customized to the organization/community.]

FACILITATOR: Wow, we've just learned that Worldwide Global, Inc. is The Void's primary target, and they're wreaking havoc on our company. They're trying to illegally transfer our money, sending customers fraudulent invoices, and threatening extortion. They've also disabled our website, which means that we have no way of communicating with our clients and customers. At this point, the most important questions that we need to address are:

- ***PARTICIPANT***: How would we/how would you detect malicious activity of unknown origin on our systems?
- ***PARTICIPANT***: How would we/how would you quickly respond to a suspected cyber attack?

As you discuss these questions in your groups, you may also address the following related questions:

- ***DISCUSSION:*** What tools or assets do we have/do you have to assist us in detecting unauthorized activity?
    - ***ALTERNATE:*** What type of detection hardware and/or software do we use? How successful or unsuccessful has this software/hardware been in detecting and/or preventing this activity?
- ***DISCUSSION:*** How would we/how would you conduct an assessment of this situation?
    - ***ALTERNATE:*** What resources do we have or could we request for network forensics?
- ***DISCUSSION:*** Where do we receive our cyber response technical assistance?
    - ***ALTERNATE:*** Do we have plans, procedures or policies in place to access this assistance?
    - ***ALTERNATE:*** What are the needed resources and where would we get them?
    - ***ALTERNATE:*** Do our current mutual aid agreements address cyber specific resources and staff?

- ***DISCUSSION:*** Do we have a Cyber Incident Response Team? What is their composition/skill set?
  - ***ALTERNATE:*** Does our incident handler have a systems administrator, business process mindset, and understanding of the IT architecture?

[FACILITATOR instructs each table of participants to discuss each question among themselves.]

[AFTER 10 MINUTES, FACILITATOR asks a representative from each table to stand and share ONE OR TWO MAJOR AREAS OF AGREEMENT /COORDINATION, AND ONE OR TWO MAJOR AREAS OF DISAGREEMENT/CONFUSION. These are discussed with all the participants in the room and captured on paper, laptop or other media for later follow up.]

FACILITATOR: Now that we've shared our initial thoughts and discussed initial questions, let's talk about a few things that the news didn't report.

Slide 15 - Internal Issues [TIMING OF SLIDE: 5 minutes]

[Note that your company may not follow the same internal protocol described below, in which case the FACILITATOR may need to adjust as necessary to make the protocol applicable to the organization.]

FACILITATOR: What hasn't been covered by VNN is that there were also signs on our internal systems that something was amiss.

It started two weeks ago, when our security event console indicated the detection of suspicious network activities. Our system administrator conducted his daily check on the system backup server and discovered a backup error message. Upon further investigation, though, he did not find any additional errors, nor did he notice anything unusual. The system administrator logged the error message according to our standard logging procedures.

A week ago, the database server on our corporate local area network crashed. After an automatic reboot, operations appeared normal, but shortly afterwards IT Support received several phone calls from users in the Accounting Department reporting that their network appeared to be slow. By noon, additional calls were received from users in other departments, to the point where IT support became overwhelmed and considered escalating the problem to management.

In addition to those internal issues, The Void's hacking is having significant negative impacts on our business:

- As a company, our productivity has dropped significantly as a result of the cyber threat rumors and unresponsive systems
- Several of the customers who received unauthorized invoices are threatening legal action
- Wary of what they perceive as unsecure systems, customers and stakeholders alike are refraining from making any investments in our company

As we move to the discussion part of this inject, focus on the ways we'd notify stakeholders and share information to combat this attack.

Are there any questions before we begin brainstorming and discussion?

[RESPOND TO QUESTIONS]

Slide 16 - Discussion 2 – Notifications and Stakeholder Communications [TIMING OF SLIDE: 25 minutes]

[FACILITATOR LEADS discussion. In addition to these questions, FACILITATOR can prompt the participants with more specific questions customized to the organization/community.]

FACILITATOR: The situation at Worldwide Global, Inc. has reached a crescendo, with significant negative impacts on our employees and customers. At this point, the most important questions that we need to address are:

- ***PARTICIPANT***: Who would we, or who should we notify – internally and externally – in the case of a cyber event? What should these processes be?
- ***PARTICIPANT***: How would we, or how should we quickly communicate with key stakeholders to minimize the impact of a cyber event on our business?

As you discuss these questions in your groups, you may also address the following related questions:

- ***DISCUSSION:*** What is our planned decision-making process for protective actions in a cyber incident? What options are available? Planned for? How are they activated?
    - ***DISCUSSION:*** What about planned notifications? How do we do this internal to our organization? External to our organization?
        - ***ALTERNATE:*** At what point would we – or should we – contact law enforcement?
        - ***ALTERNATE:*** At what point would information be shared with vendors for possible patches?
        - ***ALTERNATE:*** Would knowledgeable experts be involved? Would the United States Computer Emergency Readiness Team (US-CERT) be notified or involved?
        - ***ALTERNATE:*** Would this situation trigger contact with regulators? Elected officials? Why or why not?
        - ***ALTERNATE:*** How would we inform our other stakeholders, including customers?

- ***DISCUSSION:*** What are the business implications of the scenario? How would we determine them?

- ***DISCUSSION:*** What are the expectations or plans for information sharing among stakeholders and response partners?

  - ***ALTERNATE:*** Are IT and business continuity functions coordinated with physical security? Would all three then be collaborating with public relations, human resources, and legal departments?

  - ***ALTERNATE:*** What internal and external messages would need to be developed? How are they being distributed? Who leads the public information process?

[FACILITATOR instructs each table of participants to discuss each question among themselves.]

[AFTER 10 MINUTES, FACILITATOR asks a representative from each table to stand and share ONE OR TWO MAJOR AREAS OF AGREEMENT /COORDINATION, AND ONE OR TWO MAJOR AREAS OF DISAGREEMENT/CONFUSION. These are discussed with all the participants in the room and captured on paper, laptop or other media for later follow up.]

Slide 17 - Break: [TIMING OF SLIDE: 15 minutes]

FACILITATOR: Thank you everyone. At this time we’re going to take a fifteen minute break, during which time I’ll again be looking to capture our best thoughts and feedback. If you have any additional ideas for this module that you’d like to share, feel free to let me know during this time. You can also use this time to grab a quick refreshment or restroom break if you need to. We will resume promptly at [INSERT TIME].

Slide 18 - Module #3: [TIMING OF SLIDE: 1 minute]

FACILITATOR: We’ve now arrived at the third and final module. As you’ll see in this VNN report, even though The Void has been stopped, Worldwide Global, Inc. is still dealing with significant fallout from the attack, including losses in revenue, layoffs and decreased customer confidence.

While watching this, think about what we should change in the future. How can we make adjustments to our plans and systems now to avoid this type of devastating attack in the future?

Fasten your seatbelts, because this is going to be a very bumpy ride for Worldwide Global, Inc.

Slide 19 - VNN Inject #3: [TIMING OF VIDEO: 5 minutes]

Please see VNN Inject Script #3 for details.

Slide 20 - Attack Timeline: [TIMING OF SLIDE: 3 minutes]

FACILITATOR: Just to quickly pull it all together for everyone, we've been at this for about eight weeks now. It all started with a general threat warning issued by The Void, saying that they'd be attacking U.S. interests with 'zero day' attacks. Then, we at Worldwide Global, Inc. conducted a security audit that uncovered a terminated employee with system access. A week later, an employee found a USB drive in the parking garage and proceeded to use it. Unbeknownst to the employee, the USB drive was used by The Void to create a backdoor into our networks.

Things started to fall apart from here, as our employees started receiving and opening phishing emails from The Void; the database server crashed resulting in a slow network and slow productivity; several attempts to illegally transfer our money were made; and false invoices were distributed to a number of our global clients. And it didn't stop there. To add insult to injury, the hackers sent an email indicating that the company's network had been infiltrated and various components taken over; threatened to cripple the company's network and expose proprietary company data unless they received $1 million; and, finally, brought our website down, crippling our ability to communicate with each other and our customers.

Thankfully, through close collaboration with law enforcement and security consultants, we were able to stop the attack, but not before it caused significant damage to our business, in the form of layoffs, profit losses, and our CEO's resignation.

In the attack's aftermath, we are revamping our policies and procedures to mitigate future attacks and losses.

Slide 21 - Discussion 1 – Assessment [TIMING OF SLIDE: 25 minutes]

[FACILITATOR LEADS discussion. We recommend emphasizing to the participants that this discussion will be focused on ways Worldwide Global, Inc. should move forward in recovering from this cyber event. In addition to these questions, FACILITATOR can prompt the participants with more specific questions customized to the organization/community.]

FACILITATOR: So we now know that all of our worst fears have pretty much been confirmed. Our CEO has resigned, our stocks have plummeted and we've been forced to make layoffs – all extremely serious implications from the attack. And we also have a picture of how The Void orchestrated their attack.

With this clearer perspective, let's take a few moments to consider one key question:

- ***PARTICIPANT***: How can we clean up our image to our internal and external audiences after a situation like this? How do we regain their trust?

As you discuss this question in your groups, you may also address the following related questions:

- ***DISCUSSION:*** What happened? How did we fall short?
    - ***ALTERNATE:*** What gaps can we identify from the occurrences that have happened?
- ***DISCUSSION:*** How can we repair the damage done to our relationships with our internal and external audiences?
    - ***DISCUSSION:*** Internally, how can we retain our employees? How can we reassure them when there have been layoffs and the company has experienced significant financial losses?
    - ***DISCUSSION:*** Externally, how should we go about regaining our customers' confidence? How can we get those who may have left us to come back? How does this impact new business in the future?
- ***DISCUSSION:*** What does Worldwide Global, Inc. need to change?
    - ***DISCUSSION:*** How do we properly arm or prepare ourselves for a situation like this cyber event?
    - ***ALTERNATE:*** What in our current process needs to be modified, removed or improved?
    - ***ALTERNATE:*** What new or different resources do we now need in order to improve our emergency planning/response process?
    - ***ALTERNATE:*** How do we ensure that we're not just protecting ourselves, but our constituents and stakeholders as well?
    - ***ALTERNATE:*** In what ways can we prepare our external audiences for a situation like this, in an effort to minimize the amount of damages or losses?

[FACILITATOR instructs each table of participants to discuss each question among themselves.]

[AFTER 10 MINUTES, FACILITATOR asks a representative from each table to stand and share ONE OR TWO MAJOR AREAS OF AGREEMENT /COORDINATION, AND ONE OR TWO MAJOR AREAS OF DISAGREEMENT/CONFUSION. These are discussed with all the participants in the room and captured on paper, laptop or other media for later follow up.]

Slide 22 - Discussion 2 – Our Way Forward [TIMING OF SLIDE: 25 minutes]

[FACILITATOR LEADS discussion. As this slide serves as the exercise hotwash, we recommend emphasizing to the participants that the focus of this discussion will be on their real-world company's way forward after participating in this TTX. In addition to these questions, FACILITATOR can prompt the participants with more specific questions customized to the organization/community.]

FACILITATOR: At this point, let's step out of our role at Worldwide Global, Inc., and consider what would have happened if it had been our organization in this situation. Specifically, let's examine the following question:

- ***PARTICIPANT***: How can we improve our training programs so that we are better prepared for a cyber attack in the future?

Specifically, you may want to consider the following questions:

- ***DISCUSSION:*** What types of training programs could we implement to ensure all of our people are better prepared?
  - ***ALTERNATE:*** How often should this training be provided? Should it be mandatory?
  - ***ALTERNATE:*** What should be the training process for new employees prior to them accessing our information system?
- ***DISCUSSION:*** How can we use training to ensure that our people understand:
  - ***DISCUSSION:*** Cyber security roles and responsibilities?
  - ***ALTERNATE:*** Our password procedures and requirements?
  - ***ALTERNATE:*** Our formal and informal policies pertaining to removable storage devices?
  - ***DISCUSSION***: What constitutes suspicious cyber security activities or incidents?
  - ***DISCUSSION:*** Whom to contact and how to report suspected or suspicious activities?

Finally, as we wrap-up today's exercise, let's do a quick hotwash. We've all now dedicated several hours to this, and I think we've uncovered some really important insights. So I'd love your help in answering one final key question. Remember, by sharing, we have the opportunity to not only help ourselves be more prepared, but also to impact changes that will improve the entire nation's resiliency.

  - ***PARTICIPANT***: What lessons did we learn today that we'd like to share, both to help our own company, and also the larger whole community?

[FACILITATOR instructs each table of participants to discuss each question among themselves.]

[AFTER 10 MINUTES, FACILITATOR asks a representative from each table to stand and share ONE OR TWO MAJOR AREAS OF AGREEMENT /COORDINATION, AND ONE OR TWO MAJOR AREAS OF DISAGREEMENT/CONFUSION. These are discussed with all the participants in the room and captured on paper, laptop or other media for later follow up.]

Slide 23 - Sharing with the Whole Community: [TIMING OF SLIDE: 1 minute]

FACILITATOR:

The exercise has now concluded – thank you all for your active participation! I think we have identified some really important insights that can help our company, and the nation, be more prepared.

So where do we go from here? As I mentioned earlier, after NLE 2012, FEMA will be using the key learnings and outcomes from the exercise to revise our nation's cyber security plans. If we'd like, that could include our tabletop exercise today, making us a small but impactful piece of the puzzle for change.

If that is something that we'd like to do, I can compile the ideas that we identified today and submit them via the collaboration site at http://www.fema.gov/plan/nle. Alternately, if you'd prefer to share individually, I'm happy to email around this link, as well as the list of ten questions that FEMA has asked us to focus on, for those who would like them.

If we'd prefer to keep our learnings internal, then that is fine as well, and I am happy to compile them so that they can be integrated into any future plans that we develop.

Slide 24 - Additional Resources: [TIMING OF SLIDE: 2 minutes]

FACILITATOR: For those who would like to learn more about the cyber security topics discussed today, feel free to visit any of the following resources listed here on the screen, including:

- FEMA's website – http://www.fema.gov
- FEMA Private Sector Division's website – http://www.fema.gov/privatesector
- NLE 2012 website – http://www.fema.gov/plan/nle/index.shtm
- NLE 2012 private sector participation guide – http://www.fema.gov/library/viewRecord.do?fromSearch=fromsearch&id=5628
- DHS' cyber security website – http://www.dhs.gov/files/cybersecurity.shtm
- DHS' Stop. Think. Connect. Campaign website – http://www.dhs.gov/files/events/stop-think-connect.shtm
- FEMA's whole community website – http://fema.gov/about/wholecommunity
- US CERT – http://www.us-cert.gov
- National Response Framework (NRF) – http://www.fema.gov/emergency/nrf
- NRF Cyber Incident Annex - http://www.learningservices.us/pdf/emergency/nrf/nrp_cyberincidentannex.pdf

Again, thank you all very much for your active participation in today's exercise. If you have any questions or comments that you'd like to share, please don't hesitate to reach out to me at any time or to the FEMA Private Sector Division directly at FEMA-Private-Sector@dhs.gov.

Thank you!