**"Greetings" from The Void:
Communicating While Under Cyber Attack**

**Draft of Workshop for Feb. 17, 2018**

**Dr. Waleed Farag, IUP Professor
Dr. Ben Rafoth, IUP Professor and Director of the Writing Center**

**Adapted from the National Level Exercise 2012 developed**

**by the Federal Emergency Management Agency (FEMA)**

**Cyber Security Table Top Exercise**

**Introduction**

A Tabletop Exercise is a discussion-based exercise, facilitated by a discussion leader and based on a given scenario. The exercise is designed to help evaluate an organization’s communication response plans and procedures. For today’s purposes, participants will decide on information to be shared with the public and convey ideas to the organization’s Communications Director. The rationale for this exercise is based on the fact that when a cyber incident occurs, clear and accurate communication within and between stakeholders and the general public is an essential part of resolving the crisis. Today's exercise will help participants to experience the importance of communicating clear and accurate information.

**FACILITATOR FOR SLIDES 1-8: WALEED FARAG**

**Slide 1 –Welcome:** Waleed introduces himself as an IT expert and will discuss the rationale for this activity and how it simulates the environment in which IT professionals like him must respond to cyber incidents.

**Slide 2 -** Agenda Review

Waleed: Before I walk you through the agenda, let’s all introduce ourselves.

[Ben introduces himself.]

[Participants introduce themselves to other members of their tables.]

Waleed: 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 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. Our task will be to serve as IT professionals who are writing a communique to the Communications Director about what has transpired.

**Slide 3 – What is a cyber incident?:** A cyber incident is a past, ongoing, or threatened intrusion, disruption, or other event that impairs or is likely to impair the confidentiality, integrity, or availability of electronic information, information systems, services, or networks.

**Slide 4 – Incident handling process:**

* Preparation: Maintaining and improving incident response capabilities and preventing incidents by ensuring that systems, networks, and applications are sufficiently secure.
* Identification: Confirming, characterizing, classifying, categorizing, scoping, and prioritizing

suspected incidents;

* Containment: Minimizing loss, theft of information, or service disruption;
* Eradication: Eliminating the threat;
* Recovery: Restoring computing services quickly and securely; and communicating with those affected by the incident
* Post-incident activities: Assessing response to better handle future incidents through utilization of reports, “Lessons Learned,” and after-action activities, or mitigation of exploited weaknesses to prevent similar incidents from occurring in the future.

**Slide 5 – Exercise overview – Goals:** The main goal for today is:

* To provide clear, accurate, and appropriate input to the organization’s Communications Director for the purpose of information sharing with the broader organization and the general public;
* To experience the pressure, uncertainty, and fluidity that characterizes communicating during a cyber incident;
* To view communication as situation-based and to practice responding to a situation that depends on the accuracy, clarity, and conciseness of the communique.

**Slide 6 – Exercise overview – Ground Rules:**

To ensure today’s table top exercise is as productive as possible, there are a few ground rules. Please keep in mind the following:

* There are no right or wrong answers. The levels of cybersecurity familiarity and expertise here in this room vary widely, from little or none to advanced. However, all ideas are welcome.
* Choose one member of your group to write a communique to the company’s Communications Director. Choose another member to present the communique to everyone in the room. Everyone in each group should make notes for him/herself as needed. The notes you take will become the communique you send to the Communications Director.
* The Communications Director will use the information in the communique to write announcements for the public and press releases for the press. Note: A Press Release is a document written by the Communications Director and posted on the company’s website for the public to see. It is also sent to various news outlets. Information in the release is also e-mailed company-wide to all employees. The Communications Director relies on the computer experts to feed him information he can understand and release to the public (or not). In the release, he will need to decide how to describe what happened, what its consequences have been, what the company is doing now, and what that company will be doing going forward. Of course, some information must also remain confidential, and part of your job is to help the Communications Director decide what information can be made public and what cannot.

**Slide 7 – A company under attack**: We are now about to start the exercise.

For the duration of the exercise, our simulated company will be known as Worldwide Global, Inc.

A network of hacktivists known as The Void threatened to unleash, and I’m quoting here, “a global day of extreme action against U.S. interests and organizations, both private and government-related.” That’s an attack which exploits computer system vulnerabilities unknown to others, even the software developer. There are indications that The Void may have already gained access to the systems they’re going to exploit.

We have just learned over night that hacktivists are acting on their threats – and their target is us, Worldwide Global. From fake invoices to extortion threats, it seems that The Void has managed to work its way deep into this company’s networks.

We are now going to watch a video. 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 would be taking as we try to respond to and stop the attack. And think about the information we will share and the information we will keep confidential.

Also, pay attention to their use of the words “hacker” and “hacktivist.” As IT professionals, we want to use better terms than the news anchor does, so we will use the term “threat actor,” which is the FBI’s term and commonplace among cybersecurity professionals.

**FACILITATOR FOR SLIDES 8-13: BEN**

**Slide 8 – News cast:**

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?

We are now going to play the video. Keep in mind that your specific tasks today are: (1) to understand, as best you can in the limited amount of time available, the nature and scope of the attack and the resources available to you, and (2) to provide information to the Communications Director to be used for press releases to the rest of the company and to the public. To accomplish these tasks, you are asked to put yourself into the situation – to think, listen, speak, and write as if you are part of Worldwide Global, Inc.

You should also plan to take copious notes from here until the end of today’s activity. Remember, these notes will become the basis for your communique to the Communications Director.

BEN: PLEASE PRESS PLAY ON NEWSCAST

**Slide 9 – Discussion**

Wow, overnight we learned that Worldwide Global, Inc. is The Void’s primary target, and they are wreaking havoc on our company. They are trying to illegally transfer our money, sending customers fraudulent invoices, and threatening extortion. They have also disabled our website, which means that we have no way of communicating with our clients and customers.

At this point, the most important question that we need to address is this: How would we/how would you quickly respond to a suspected cyber attack?

**Slide 10 - Discussion**

Here are a few other questions to think about:

Does the organization have a Cyber Incident Response Team? What is their composition/skill set?

Who would you, or who should you notify – internally and externally – in the case of a cyber event? What should these processes be?

How would you, or how should you quickly communicate with key stakeholders to minimize the impact of a cyber event on the your business?

**Slide 11 – In-Depth Discussion (10 minutes)**

Discussion: Each table will choose ONE discussion question.

Ben will explain that after 5 minutes, we will ask a representative from each table to stand and share one or two major areas of agreement that resulted from discussing the question. Remember to take notes.

Question 1: What are the expectations or plans for information sharing among stakeholders and response partners?

Question 2: What are the business implications of the scenario? In terms of IT, are they secondary to dealing with the cyber attack?

Question 3: What internal and external messages would need to be developed? How are these messages being distributed? Who coordinates the gathering of technical information before it goes to the Communications Director?

Ben will instruct each table of participants to discuss the question among themselves. After 5 minutes, Ben will ask a representative from each table to stand and share one or two major areas of agreement that resulted from discussing the question.

**Part 2: Write Communique**

**Slide 12 – WRITE YOUR COMMUNIQUE**

Ben: now it is time to write your communique to the Communications Director.

We will project the memo template.

Ben will instruct groups that they have 15 minutes to write. After 15 minutes, they will share their communique with the Communications Director and receive his response.

MEMO TEMPLATE:

Worldwide Global, Inc.

Internal Communique

TO: Mr. Waleed Farag, Communications Director

FROM:

DATE & TIME:

SUBJECT: Cyber attack information

In response to your recent questions, “What information must be released company-wide and to the general public? What information must be shared with the Communications Director but should not be released beyond that?” the IT Department is able to provide you with the following information.

Ben: As groups are working, say, “What hasn’t been covered by VNN is that there were also signs on our internal systems that something was amiss. You will now receive new information that we have received about the nature of this attack and its impact on our business.”

Ben will hand out notecards with new information as each group is working.

 **Notecard 1:** It started two weeks ago, when our security event console detected 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 found no additional errors and noticed nothing unusual. He logged the error message according to standard logging procedures.

**Notecard 2:** 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.

**Notecard 3:** E-mail message from the company CEO: “Our productivity has dropped significantly as a result of the cyber threat rumors and unresponsive systems. I want this problem resolved asap.”

**Notecard 4:** Text message from company’s legal department: “Customers who received unauthorized invoices are threatening legal action. Is anything being done about this??”

**Notecard 5:** Phone call to IT Department from the company’s Chief Financial Officer: “Customers and investors are losing confidence in our systems not buying our products or investing in our company. This is a disaster!”

**Part 3: Reports and Communications Director Response**

**Slide 13 – REPORTS AND COMMUNICATION DIRECTOR RESPONSE**: Ben: groups will now share their reports with the Communications Director and receive feedback. Please read your report aloud.

Waleed: As the Communications Director, I will now respond to your reports. [Waleed will give feedback.]

**Part 4: Conclusion and Wrap-Up:** The Aftermath of the Attack

**Slide 14 – The Aftermath:**

 Ben: We are now nearing the end of the exercise. 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? How can we improve the lines of communication between IT, the Communications Director, and our various stakeholders?

One thing we know: The foreseeable future is going to be a very bumpy ride for Worldwide Global, Inc.

PLAY VIDEO SLIDE 14

**Slide 15 – RESOURCES** Waleed: explain additional resources

**Slide 16 - Thank you!**