**Introduction**

* MITRE – Cyber Exercise Playbook / NIST 800-84
* Paper-driven exercise with injects scripted by exercise planners and delivered via paper (Cards / Discussion)
* **Purpose** to practice incident response procedures related to Information Security in order to identify potential weakness in people, process, and technology.
* **Objective** Expose weakness, assess communication, find data source gaps, and measure training effectiveness.

**Assumptions**

* IR platform is operational
* Can utilize the CSIRT handbook
* Normal team facilities are available
* Questions can be asked but not all questions can be answered
* Facilitator 1 and Facilitator 2 are at an offsite work event and are not easily accessible
* Anyone can be involved.

**06:00-09:00 AM (Slide 1)**

* It’s Friday morning and everything seems to be business as usual.
* The Corporate Marketing Services Team is tasked with putting out the ACME’s communications through various social media services.
* Logins are done from staff work machines and home machines, as some social media sites are blocked at work. Logins are also done at various branch locations. They utilize the corporate network as well as acmeremotedesktop.com to do this.

**06:00-09:00 AM (Slide 1a)**

* The Information Security Team starts arriving and the SOC is being pulled up.
* During the morning activates it is noticed that an FS-ISAC member sent the following message.
* Email Subject: [CyberIntel Confidential] ACME Corporation theme Loki Malspam
* (Link to email Screen Shot)
* Handout given

**09:24 AM (Slide 2)**

* A Marketing Communications Consultant sits down and finally has time to go through various messages from the “Contact Us” page on the ACME’s website.
* One message is cause for concern.
* The message reads “Stop sending me all of these obscene messages, or I will call the police!”
* They have left no email address or phone number to contact them.
* A note is made to look into it in the future.

**09:32 AM (Slide 3)**

* The Marketing Communications Consultant begins to receive many more of these types of messages through various forms (email and social media) after receiving these the messages they decide to escalate to the Senior Marketing Communications Specialist.

**10:29 AM (Slide 4)**

* InfoSec receives notice of the messages from the Senior Marketing Communications Specialist and begins to investigate the problem.
* What actions did you take?
* What core InfoSec principles are being affected (CIA)?
* What other teams do you get involved at this point?
* What do you do next?

**11:30 AM (Slide 5y)**

* CIO <Insert name> and CEO <Insert name> were leaving the Home Office to go visit the Westside location when they were stopped <local report> of <local TV station>
* “What is the extent of the cyber-attack that has taken place? Has sensitive company and customer data been breached?!” demands the reporter towards CEO <Insert name>.
* CIO <Insert name> and CEO <Insert name> told the reporters that they have no comment and continue walking to their car.

**11:30 AM (Slide 5n)**

* CIO <Insert name> and CEO <Insert name> were leaving the Home Office to go visit the Westside location when they were stopped <local report> of <local TV station>
* “What is the extent of the cyber-attack that has taken place? Has sensitive company and customer data been breached?!” demands the reporter towards CEO <Insert name>.
* CIO <Insert name> and CEO <Insert name> told the reporters that they have no comment and continue walking to their car.

**11:31 AM Track A (Slide 6 Positive)**

* CEO <Insert name> calls InfoSec and tells them “Thanks for the heads up. News knows about the situation. Keep me updated.”
* InfoSec VP <Insert name> is currently on a flight to India and will not be reachable for the next 8 hours. CISO <Insert name> is currently on vacation and cannot be reached.
* What actions did you take?
* What core InfoSec principles are being affected (CIA)?
* What teams have you involved this far?
* What do you do next?

**11:31 AM Track B (Slide 6 Negative)**

* CEO <Insert name> calls InfoSec and tells them to look into and fix the problem as fast as possible. No excuses.
* InfoSec VP <Insert name> is currently on a flight to India and will not be reachable for the next 8 hours. CISO <Insert name> is currently on vacation and cannot be reached.
* What actions did you take?
* What core InfoSec principles are being affected (CIA)?
* What teams have been involved this far?
* What do you do next?

**11:41 AM (Slide 7 Positive)**

* It has been determined that the ACME accounts for Facebook and Twitter have been comprised.
* It has also been determined that the ACME Instagram account has not been comprised.
* This is because 2FA was set for the ACME Instagram account.
* What would you do with this information?

**11:41 AM (Slide 7 Negative)**

* It has been determined that the ACME accounts for Facebook and Twitter have been comprised.
* It has also been determined that the ACME Instagram account has not been comprised.
* What would you do with this information?

**12:30 PM (Slide 8)**

* InfoSec has gone through IDS alerts, NetFlow records, and searched through logs, however nothing was out of the ordinary except for two things.
* One of the employee’s laptops show an abnormal amount of outbound traffic to various social media accounts via NetFlow records. The time of these logs indicate that they were at the Columbus branch office and were directly connected to ACME’s network.
* SIEM alerts for malware outbreak? Which is potentially affecting the availability of Customer Facing Website, users can not login to acme.com.
* Confirmed that core backend technology is down, and is not repairable for the foreseeable future.
* What actions did you take?
* What core InfoSec principles are being affected (CIA)?
* What other teams do you get involved at this point?
* What do you do next?

**12:31 PM Paper Info Drop (Slide 9 Yes)**

* Handouts given. *One to each team.*
* What actions did you take?
* What core InfoSec principles are being affected (CIA)?
* What other teams do you get involved at this point?
* What do you do next?

**12:31 PM** **Info Drop (Slide 9 No)**

* Display alerts on screen.
* What actions did you take?
* What core InfoSec principles are being affected (CIA)?
* What other teams do you get involved at this point?
* What do you do next?

**12:56 PM (Slide Social A)**

* Alert from physical security that the employee Norman Shady badged into the home office at 8:06 and Norman Shady badged into the Columbus office at 8:14.
* Norman Shady is currently at New Employee Orientation (NEO)
* Norman Shady is part of the Social Media Team.
* Norman Shady left documents on his desk at the Columbus branch.
* What actions did you take?
* What core InfoSec principles are being affected (CIA)?
* What other teams do you get involved at this point?
* What do you do next?

**12:56 PM (Slide Social Fail)**

* The accounts have been taken again. How can this be?
* What actions did you take?
* What core InfoSec principles are being affected (CIA)?
* What other teams do you get involved at this point?
* What do you do next?

**Debrief 1**

* Identify – Pros/Cons
* Protect - Pros/Cons
* Detect – Pros/Cons
* Respond – Pros/Cons
* Recover – Pros/Cons

**Debrief 2**

* Any concerns for ACME as a whole?
* Any issues with documentation?
* In what ways did the involvement of the media change the dynamics of the incident?
* How would the media have gotten involved?

**Follow Up**

* Follow up meeting date TBD
* Follow up survey
* Feel free to stay around and talk about the exercise
* Thank you. Any Questions?