Incident Management Training for IT Operations

Communications

Sprint 2

“The message is effective when the receiver understands and remembers it!”

Sprint 2 – What to Expect

- ✔ **Presentation:** *Preparation and delivery of written and verbal briefings; responding to difficult questions; how to establish timelines and time contracts; understanding span of control; overview of Unified Command*
- ✔ **Presentation:** Implementing CAN Reports and the IMS Briefing format
- ✔ **Breakout Session 2:** CAN Reports/IMS Briefings [*prepare for main session deliverables*]
- ✔ **Debrief and instructor feedback to participants**

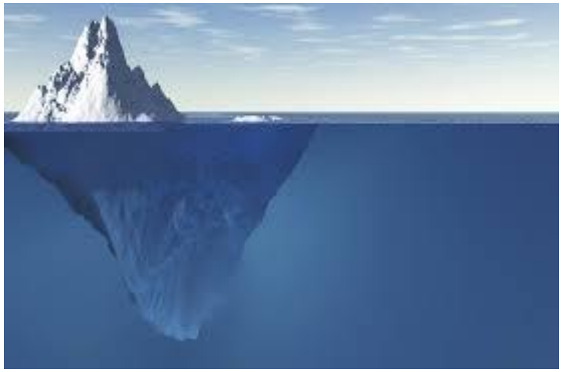
Incident Response Perspective

- Process must be in place to accept and transition from Normal Ops to Incident Ops
  Mean Time To Assemble (MTTA)
- Response is not just another meeting!
- Deliberate – Clear – Organized
- Assemble the right team at the right time to do the right things

Communications Process Review

CAN Report

- Conditions
- Actions
- Needs



- 60 seconds
- Tactical report
- Guide for thinking
- Guide for asking questions
- Clarity and updates
- Verbal or written

IMS Briefing

- Introduction
- Main Points (3)
- Summary

- 1-2 minutes
- Useful for business impact
- Non-technical
- More storytelling
- Verbal or Written

Know your audience - you are the *curator* of information

Preparation – Presentation – Post Game

CAN Reports

Conditions (past)

What was or is happening?

Actions (present)

What's being done?

Needs (future)

What are the needs?

Who gives a CAN Report?

How is it used?

When is it used?

Why is it used?

Always consider the consumer of the CAN Report before giving it!

Anatomy of a good CAN Report

@ 80-ish words

Conditions:
On March 2nd @ 22:00 PST there was a Core Production release. A script in this release led to subscribers being disconnected from the network. The amount of subscribers affected is unknown at this time (3 March 08:00 PST)

Actions: We are determining

1. which script caused the incidents
2. how many subscribers were affected by this
3. how to fix the script and rerun to restore services

Needs:

1. Provide an ETA to restore by 09:00 PST, if possible
2. Include specific checks going forward to ensure that service is not interrupted due to this again

CAN Report Practice Session

CONDITIONS

Leader is appointed or established by the group within the first 30 seconds.

ACTIONS

- Leader directs each team member to develop a <60 second CAN report on a technical topic. Leader also develops a CAN report
- Each team member and Leader delivers CAN report to the group
- At the conclusion of each CAN report, all team members offer suggestions and comments for improvement.

NEEDS: ***At the conclusion of the exercise, Leader will select a CAN report to be delivered in main session.***

Incident Management Training for IT Operations

Breakout Session 2: Can Report

IMS Briefing

Introduction

What was or is happening

Main points

Numbered

Summary

What did we tell them

Who gives an IMS briefing

How is it used?

When is it used?

Why is it used?

Always consider the consumer of the IMS briefing before giving it!

IMS Briefing: Introduction

Introduction:

This is Amy, I am the LNO for the Log4J incident at Northern Cascadia University (NCU) that began at 13:57 Pacific Standard time. This is my first briefing, expected to last one minute.

To begin, root cause is unknown and estimated time to resolution is not established.

I have two main points to share with you:

Number 1: Update on our completed incident notifications.

Number 2: Inform you that NCU incident response team is assembled and has identified this as a potential Malware incident at NCU.

IMS Briefing: Main Points

Main Points:

1. NCU IT SMEs are notified and a team of 5 incident responders is working to resolve the issue. At this time, school administration is aware of the incident and email notifications have been sent to key internal NCU stakeholders and faculty.

2. Our current working assumption is that this incident may be due to a Log4 J vulnerability: The CAS – Central Authentication System – is compromised. This is the primary authentication system for students across the entire NCU campus. The team is currently investigating logs for IOC's – indicators of compromise – to determine next steps to protect the CAS environment.

IMS Briefing: Summary

Summary:

In summary, be advised that initial notifications have been sent to key faculty and administration and the next update for that group is scheduled to be delivered via email at 14:45 Pacific Standard Time. Also, the NCU CIO was briefed.

Regarding the compromise of the CAS, I can add that the NCU SME confirm there are no secondary options to fail over the CAS login service and there is a high risk of leaving the server online. Based on our current understanding of the situation, if the server is taken offline, there will be a major service disruption.

My next update will be at 15:30 Pacific Standard Time.

Is there additional information I can provide?

Incident Management Training for IT Operations

Breakout Session 2: IMS Report

IMS Briefing Practice Session

CONDITIONS

Group Leader (GL) is selected by the members of the breakout group.

ACTIONS

- GL directs each team member to write a ≅ 200 word IMS briefing on a technical topic. GL also writes an IMS briefing.
- Each team member and GL delivers IMS briefing to the group
- At the conclusion of each IMS briefing, all team members offer suggestions and comments for improvement.

NEEDS: ***At the conclusion of the exercise, GL will select an IMS briefing to be delivered in main session (<90 seconds).***

Questions and Wrap up