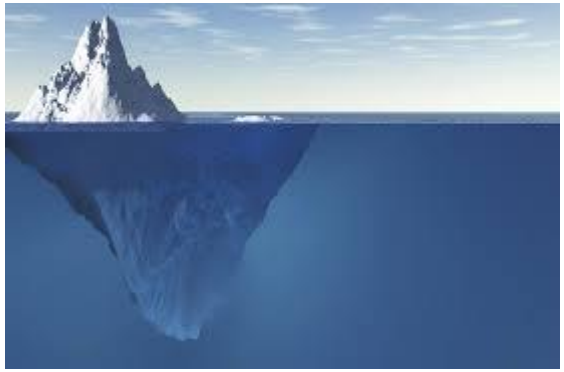
OnSite
Incident Management Training

Operational Period #2

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**

You are the *curator* of information

Anatomy of a good CAN Report

Condition: At 17:00 Hours EST, 20 applications are reporting that users located in the western part of the United States are unable to login. 2,500 users are impacted.

Actions: SREs determined that a recent code deploy broke the authentication instance accessed by these users. Rollback has been initiated and will be completed by 18:15 EST.

Needs: The Teams chat will be on hold and waiting for rollback to be completed and impacted instances rebooted.

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:

First, 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.

Second, 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?

OnSite
Incident Management Training

Breakout session #1

CAN Report Practice Session

CONDITIONS

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

ACTIONS

- GL directs each team member to develop a <60 second CAN report on a technical topic. GL also develops a CAN report
- Each team member and GL 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, GL will select a CAN report to be delivered in main session.***

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