Incident Management Training for IT Operations

Sprint 1

"Simplexity"
–Jeffrey Kluger

Sprint 1 – What To Expect

✔ **Welcome & introductions**

✔ **Presentation: Overview of the Incident Management System (IMS) and key** *roles of leadership, communication and documentation; maintaining forward momentum during the response briefings; challenges of incident leadership*

✔ **After Action Reviews**

Sprint 1 – What To Expect

✔ The general perspective of IM as a process and practice

✔ An open forum for you to ask questions of us and your fellow participants.

✔ We'll use your terminology where we can.

✔ Breakout Session 1: Operational Maturity Assessment & Discussion [*prepare for main session deliverables*]

✔ Opportunities to take on roles that may be outside your comfort zone.

✔ Direct feedback from us.

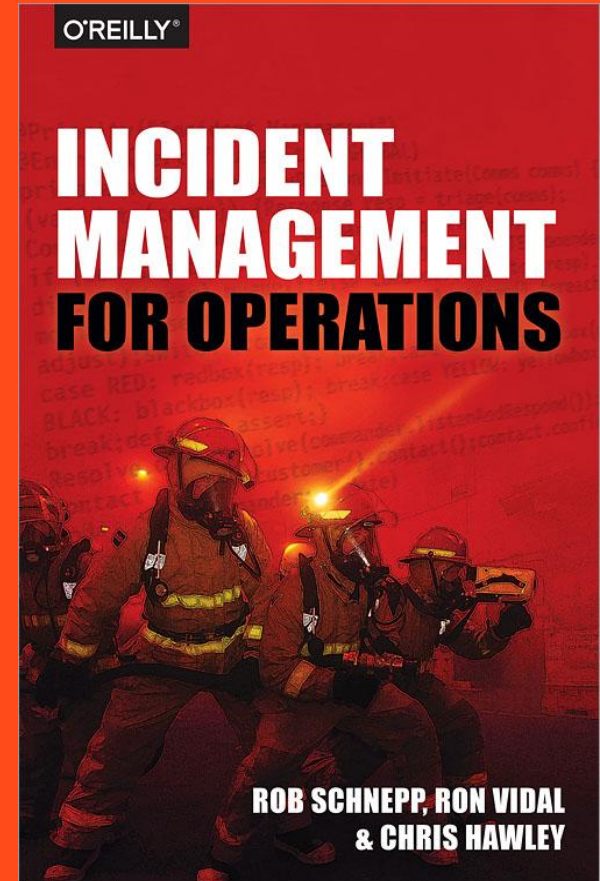# Worldwide Training

Companies that *Trust* Blackrock 3 Partners

www.blackrock3.com

Director of Operations
Ashley@blackrock3.com

Academy Resources and Instructional Content
Andy@blackrock3.com

O'REILLY®

INCIDENT MANAGEMENT FOR OPERATIONS

ROB SCHNEPP, RON VIDAL & CHRIS HAWLEY

Introductions

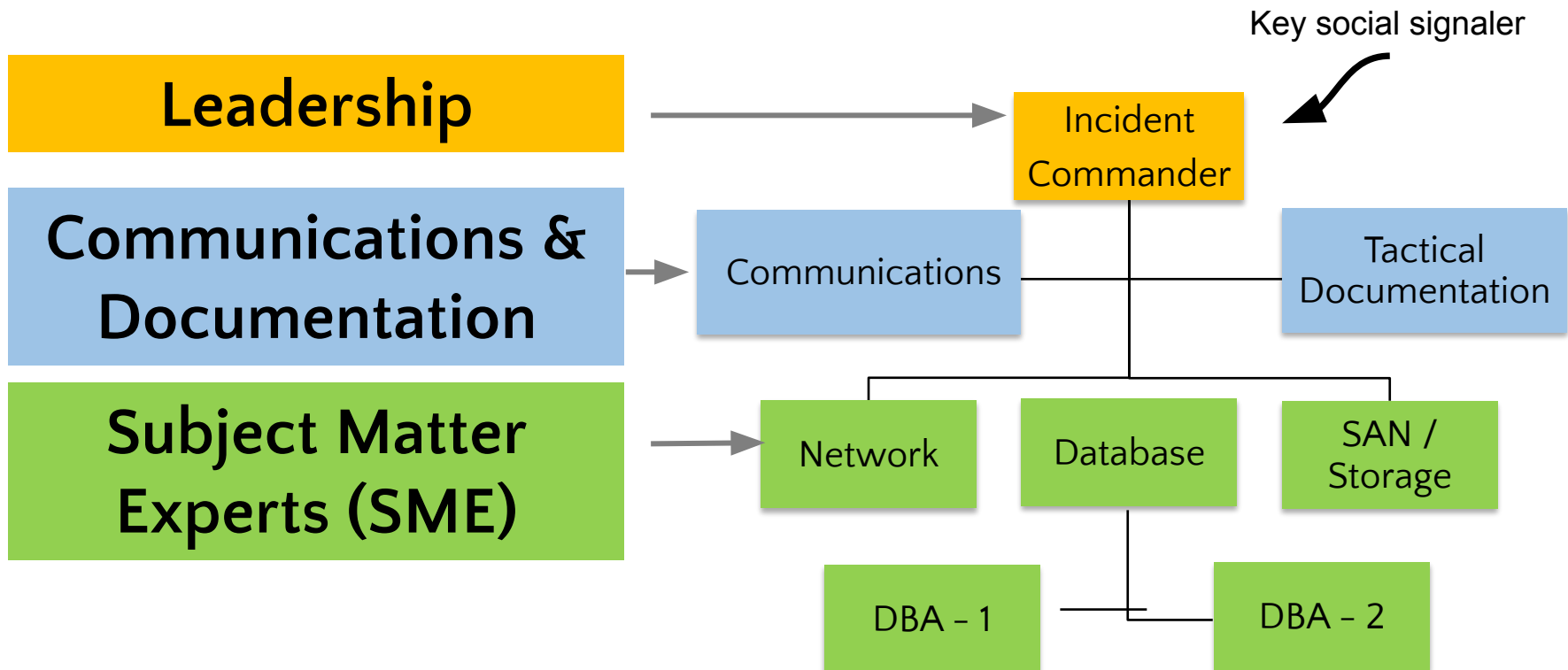*In 30 seconds or less, tell us your . . .*

- **Name**
- **Location**
- **Job Function**
- **Incident response experience**
- **Expectations for the training**

Incident Management is a Practice

Three distinct activities must occur during incident resolution

Incident Management vs. Incident Response

Key social signaler

Leadership → Incident Commander

Communications & Documentation → Communications — Tactical Documentation

Subject Matter Experts (SME) → Network — Database — SAN / Storage

DBA – 1 — DBA – 2

Building a Process

Making the Jump
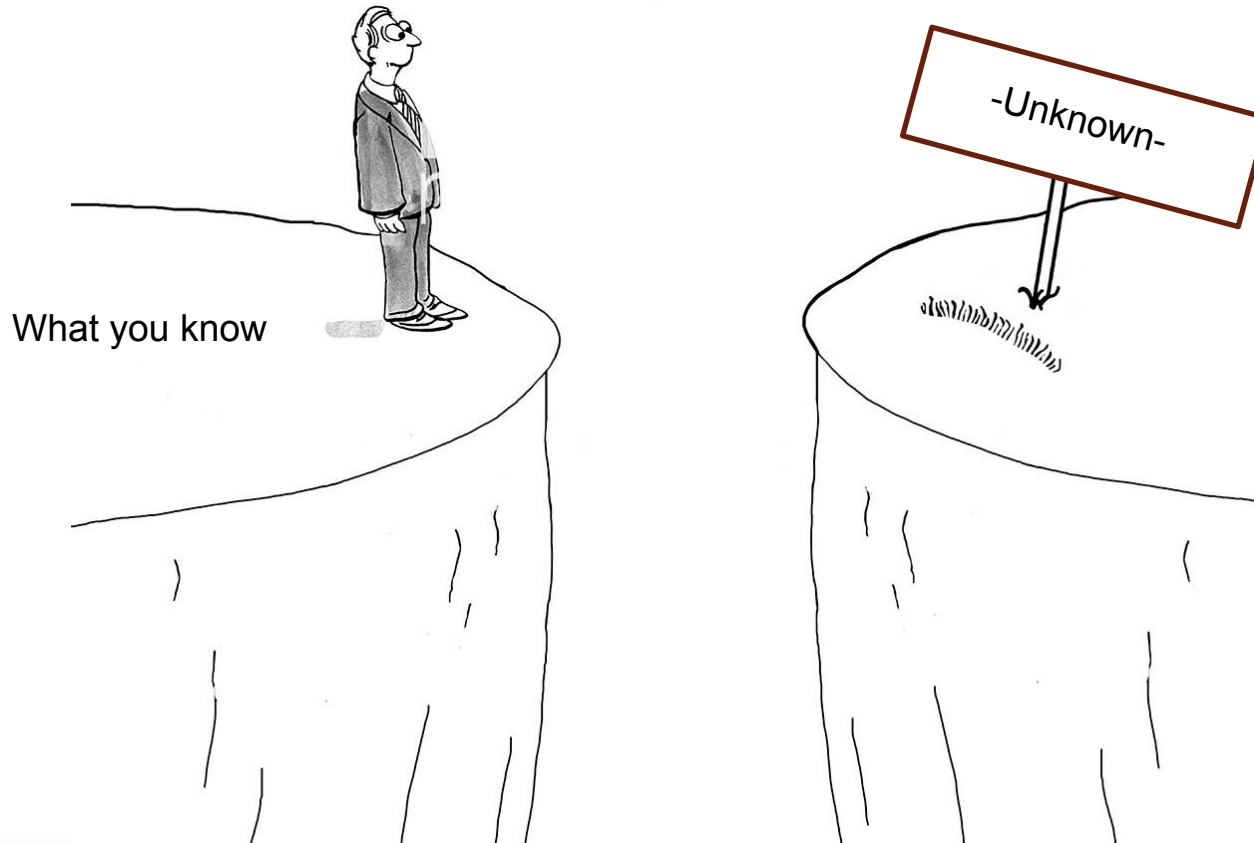
Incident Response Challenges

It's about navigating the complexity of the problem with simple understanding, *and* it depends upon when you enter the complexity

Momentum Disruptions

Uncertainty Doubt

Own the incident response process
not the problem!

Key Points

Use of the CAN report (Conditions Actions Needs)

Forward momentum

Clock management

Hailing protocol: Acknowledging communications

SME deflects a disruption

Use of the Communications (LNO)

Numbered list

Incident Documentation

Key Event #	Elapsed Time (mm:ss)	From=>To	Key Event
			North Cascadia University Log4J Incident
			4/27/22
			14:10 PST START
		Resource	**Command Staff (CS)**
		Matt	**IC** = Incident Commander
		David	**LNO** = Liaison Officer
		Kevin	**S** = Scribe
			A-Reps & Problem Solvers
		Taylor	**SC** = School Contact
		Sonic	**SME** = Subject Matter Expert
1	00:00		START: Log 4J Incident at N. Cascada Univ
2	00:21	IC=> All	Incident Bridge initiated @1410
3	00:30	IC=> All	Assigning CS positions
4	00:33	IC=> All	IC=Matt, LNO=David, S=Kevin
5	00:38	IC=> All	SC=Taylor, SME=Sonic
6	00:50	SC=>All	Log4J Attack, CAS, CIO upset
7	01:03	IC=> All	**CAN #1 - CONDITIONS:** Compromise detected at 13:57 pst at North Cascadia University. Central Authentication Server (CAS) compromised. CAS is the primary authentication service for all students. **ACTIONS:** Key roles filled and key stakeholders comtacted. Investigate nature of incidents. **NEEDS:** Collect & investigate logs. Determine next steps to protect CAS.
8	01:58	IC=>SME	Can you pull Logs? Yes
9	02:11	IC=>LNO	Add DCSIRT Log Analysis SME
10			**ADD 15 MINUTES FOR DRILL PURPOSES**
11	02;45	LNO=>IC	DCSIRT SME DeV wiLL join bridge
12	02:43	IC=>SME	Logs Avail? Yes
13	02:57	IC=>SME	Review logs & rejoin in 30min? Yes
14			**ADD 30 MINUTES FOR DRILL PURPOSES**
15	03:18	IC=>LNO	Get Business Impact in 30 minutes
16	03:48	IC=>LNO	School impact? No backup service
17	04:04	LNO=>IC	Business Impact is Major.No secondary option
18	04:10	IC=>SME	Update to log review? 10 Minutes
19	04:24		**ADD 10 MINUTES FOR DRILL PURPOSES**
20	04:30	SME=>IC	Taking system off line

Responder Toolbox

- **Rule in – Rule out**
  - Impartial decision making
- **Timelines and Time Contracts**
- **Response – Answer**
  - Unknown
  - Unable
  - Repeat
- **1 Q – 1 A**
- **Span of Control**
  - Group Leaders
- **Unified Command**

Breakout Sessions

- **Take a role that makes you uncomfortable!**
- **Use breakout rooms to practice transitions and forward momentum**
- **Screen titles for group exercises**

    Leader – Praveen

    Communications – Linda

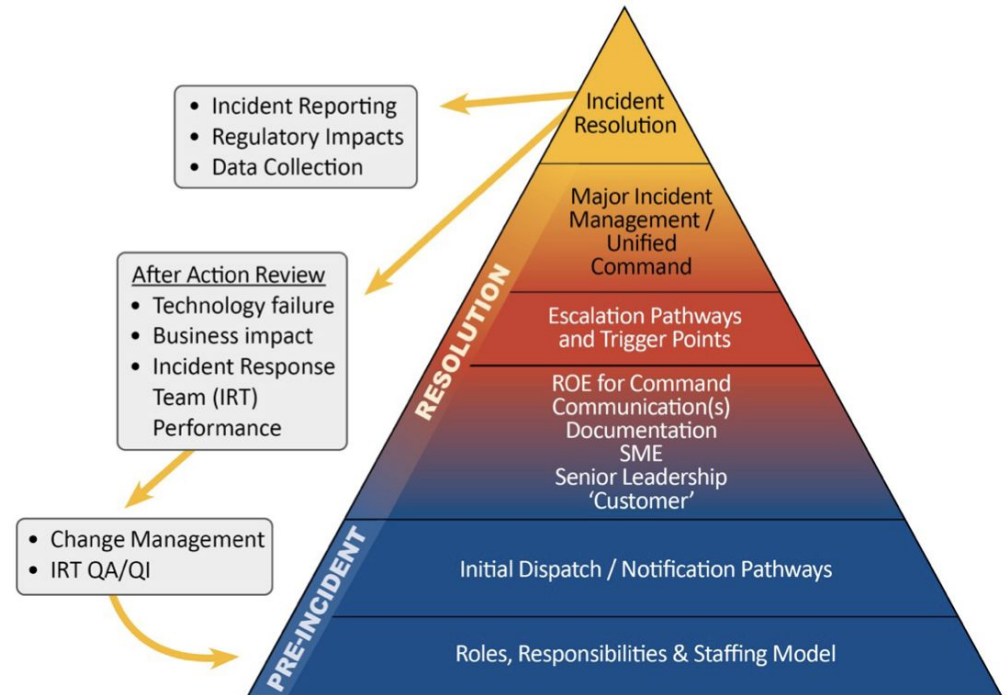   Documentation - Tyler

- **Group exercise resources:**
  https://blackrock3onlinetraining.com/academy-resources/

Incident Management Training for IT Operations

Breakout Session 1

Operational Maturity

✔ **It's a perspective on the process of incident response in your team or organization.**

✔ **Benchmarking tool**

✔ **Gap Analysis**

- Incident Reporting
- Regulatory Impacts
- Data Collection

After Action Review
- Technology failure
- Business impact
- Incident Response Team (IRT) Performance

- Change Management
- IRT QA/QI

RESOLUTION

Incident Resolution

Major Incident Management / Unified Command

Escalation Pathways and Trigger Points

ROE for Command Communication(s) Documentation SME Senior Leadership 'Customer'

PRE-INCIDENT

Initial Dispatch / Notification Pathways

Roles, Responsibilities & Staffing Model

©2021 Blackrock 3 Partners

Operational Maturity Model

Improvement Pathway for Incident Management Program

	Phase 1	Phase 2	Phase 3	Phase 4	Phase 5
Phase	Phase 1	Phase 2	Phase 3	Phase 4	Phase 5
Maturity State	Initial	Managed	Defined	Data Driven	Optimized
Descriptive State	Reactive	Responsive	Predictable	Repeatable/Scalable	Sustainable
Incident roles	• No formalized incident response (IR) training • No clear roles and responsibilities for incident management • Incident communications to key stakeholders and customers is not formalized with a recognized role	• Some level of internal on boarding for incident response • Key incident response roles implemented to some level • No clear and efficient linkage between resolution and key stakeholder communication	• Command staff functions recognized, implemented and supported by leadership • All key responders and SME's trained to a consistent standard • Regular and predictable briefing/comms cadence	• Ongoing training and exercises for all key responders • Large scale incident management in place where applicable <<Unified Command>> • Dedicated communications function assigned	• Clear plans to recruit and replace team members. • IR team may reach out to customers/key clients/other business units to assist with building joint response capabilities
Processes	No documented process for dispatch, resolver engagement, resolution or After Action Reviews	• Some level of formalized dispatch process and SLA's for key responders. • Monitoring tools integrated into situational awareness. • Blameless After Action Reviews may be completed, but not integrated in Q/A & Q/I	• On call rotations predictable and key responders assemble quickly. • Playbooks and Standard procedures developed • Accountability for performance and responder duties is clear to all	• Full support of the end to end IR process from senior leadership. • All responders accountable for performance	IR is accepted as an integral part of defending the business against financial loss, reputational risk, and loss of customer trust
Engagement	Company does not recognize or support incident response as an entity or discipline. Best efforts are relied upon from individual contributors	Mean Time to Assemble (MTTA) is unpredictable. Dispatching tools, process and accountability in place, but inefficient or outdate or inconsistently used	MTTA is optimized and repeatable for key responders to any type of incident. On call rotations are predictable.	MTTA is optimized and repeatable for Vendors, customers or any other allied responders respond as expected.	After Action Reviews fully integrated for Q/A & Q/I of the response team and the process

Overall

Low Resolution   High Resolution

Operational Maturity

CONDITIONS

Leader identified. Leader assigns the role of communications and Scribe.

ACTIONS

1. Leader directs discussion to identify different perspectives on operational maturity

2. Leader directs discussion to identify issues that prevent the incident response program from reaching optimal operational maturity. *See exercise: Improving Incident Response for further details.*

NEEDS: *Communications reports back to the main group at the assigned time. Briefing to last less than 60 seconds.*

Questions and Wrap up