OnSite
Incident Management Training

Operational Period #1

About Us

- Who We Are
  - Deep global experience in Incident Management & Critical Infrastructure
    - Fire brigades, multi-country incident response training, emergency medical services
    - Fiber Networks, Data Centers, Oil & Gas, Power, Capital Markets
- What We Do
  - Help Customer's Build World Class Incident Management Teams
    - Assess, train, and evaluate Incident Response Teams
  - Engage with Teams Across the Customer's Organization
    - NOC, Ops, Site Reliability, Cybersecurity, Support, SMEs, Executives
  - Trained, evaluated and exercised over 6,000 incident responders globally
- Who Partners With Us

Worldwide Training

Additional Resources

www.blackrock3.com

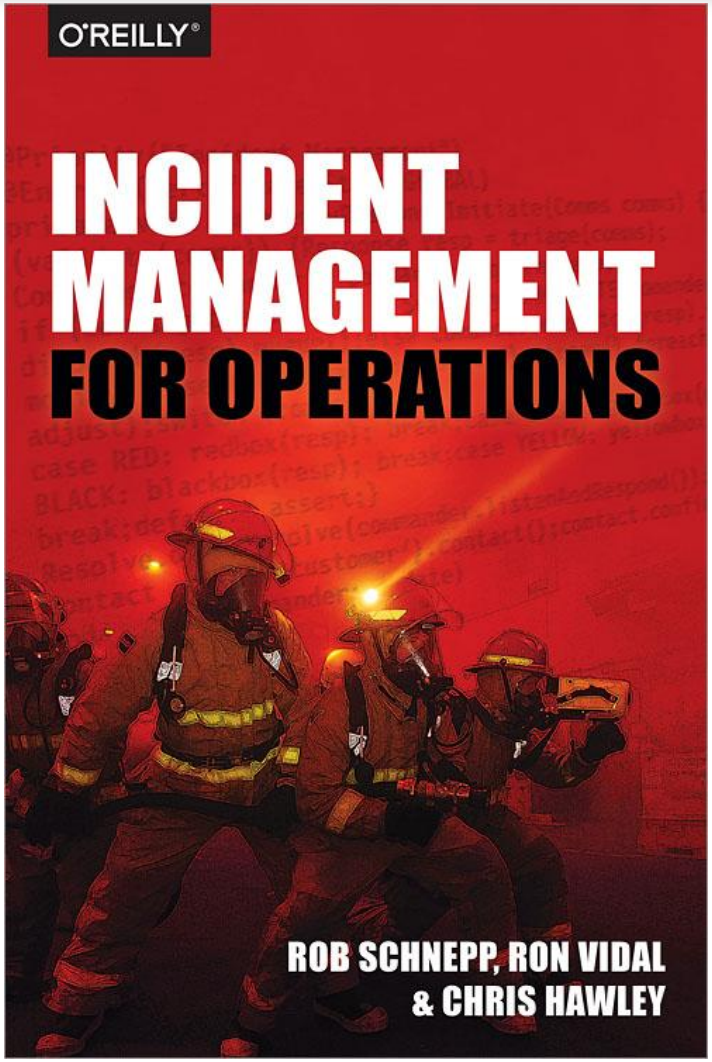
@br3guys

Rob Schnepp
Rob@blackrock3.com

Ron Vidal
Ron@blackrock3.com

Chris Hawley
Chris@blackrock3.com

San Francisco & Baltimore



Introductions

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

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

OnSite
Incident Management Training

Exercise #1 : TIME and teambuilding

TIME

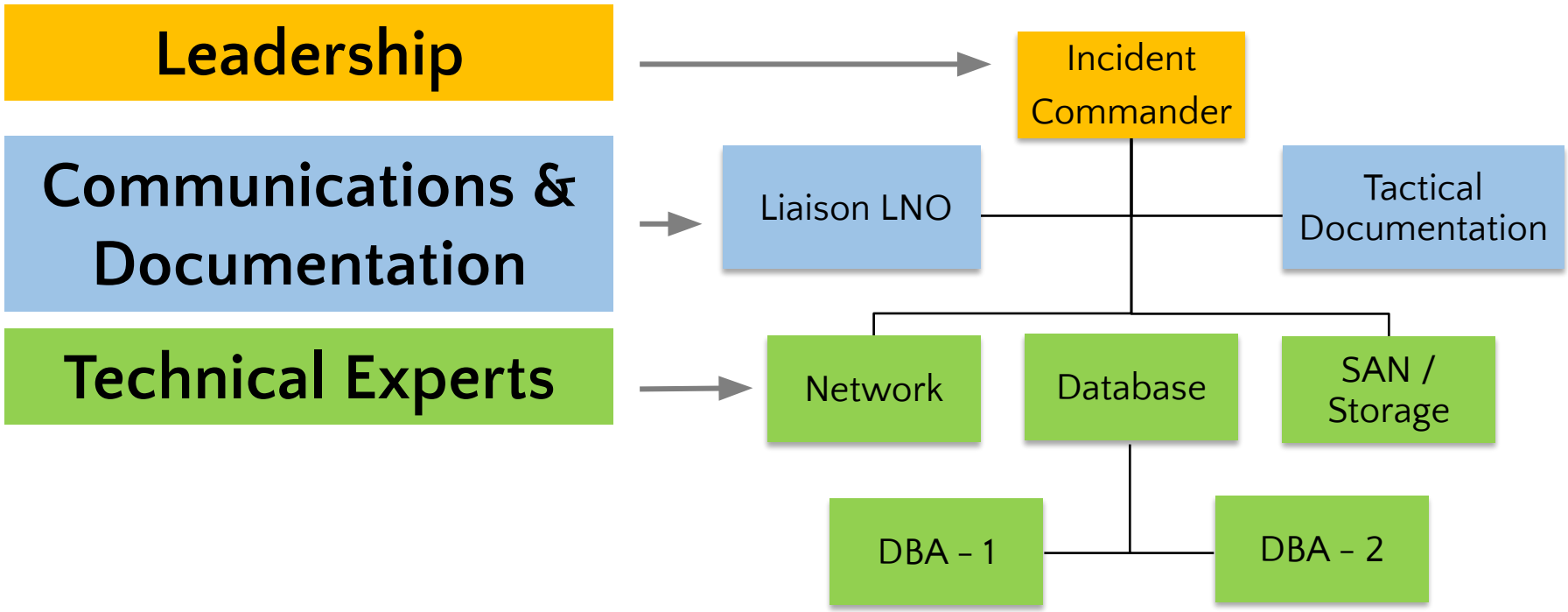
Tone
Interaction
Management
Engagement

Mean Time To Assemble
(MTTA)
is Mission Critical

Essential Activities

Three distinct activities must occur during incident resolution

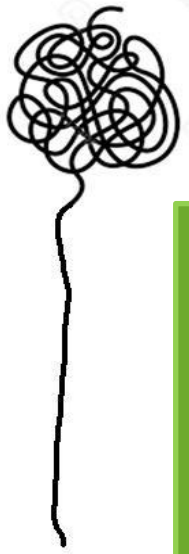
PROCESS - POSITIONS - PERFORMANCE



Incident Response Challenges

COMMAND

W
N
E
R
S
H
I
P



It's about making the best decision
in the shortest amount of time....
based on what you know at the time!

Momentum
Disruptions
Transitions

Confusion
Uncertainty
Doubt

Own the incident response process
not the problem!

Incident Response Challenges

- **Forward Momentum: Validate–Assemble–Investigate–Resolve**

  Better Worse Same

- **Minimize Disruptions: Clarity–Engaged Responders–Objectives**

  More or Different Responders

- **Deliberate Transitions: Time Contracts–Objectives–Op Periods**

  Always Have a Plan B

It's Something Until Proven Otherwise!

Incident Response Perspective

- Process must be in place to accept the rapid change 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

Benefits of IMS

Identifies roles and responsibilities

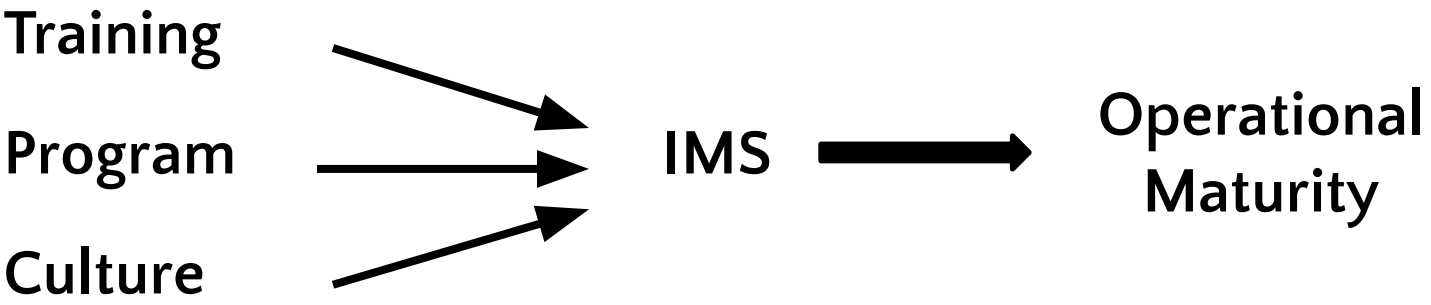
Provides the framework for command and collaboration

Identifies common terminology

Provides a framework for organized troubleshooting and decision making

Optimizes MTTA and gives the best shot at ideal MTTR

Emphasize the importance of communications



Operational Maturity Model

Improvement Pathway for Incident Management Program

Overall

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