Surviving Your First Incident

a.k.a What To Do Before You Have To Answer That Call

DON'T PANIC

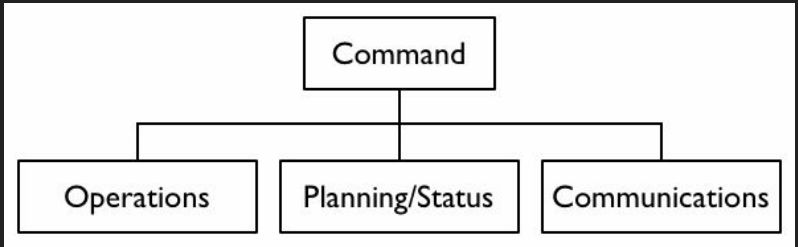
> whois bryannolen

- Worked in DFIR & Enterprise System Design/Admin for more than a decade
- Worked cases for the largest companies in the world, and some of the smallest in Australia.
- Happy to answer questions (contact details on last slide)

Welcome to The ICS - Incident Command System

Comes from California in the 1970's, by firefighters dealing with massive bushfires.

- COMMAND
- CONTROL
- COMMUNICATION



Key Roles

3 key roles,
and 2 optional lead roles:

- **Incident Manager/Coordinator/Commander**
- **Operations Lead(s)**
- **Communications Lead**

- **Legal Lead**
- **Planning Lead**

Role Breakdown - IM/IC

The Incident Manager/Coordinator/Commander OWNS the incident - all leads report to them.

They oversee the response, set priorities, delegates activities.

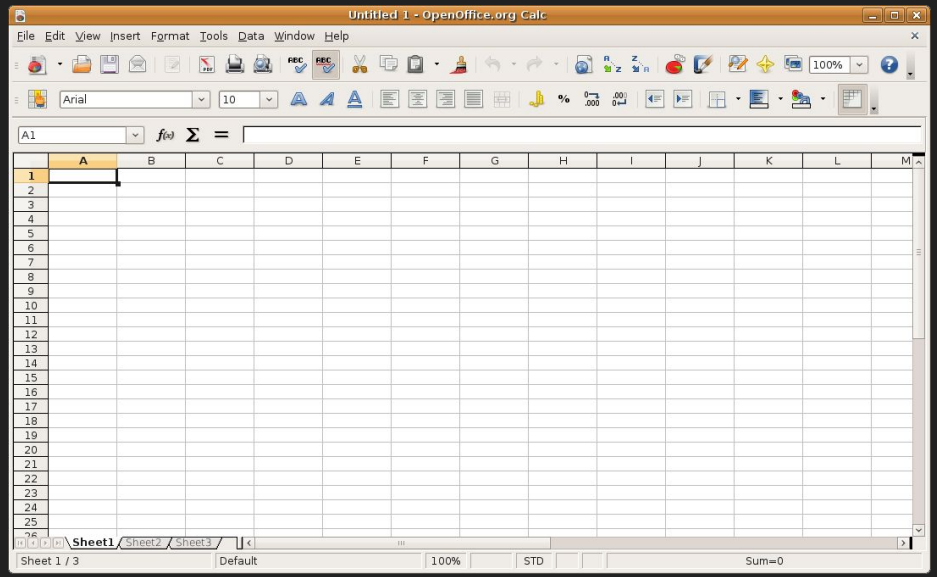
For smaller incidents, the communications lead role can be done by the IM/IC

They do not participate in the detailed analysis - they focus on the big picture/strategic.

Role Breakdown - IM/IC

[what you think IC is]

[what it actually is]



Role Breakdown - Ops Lead(s)

The Ops Lead(s) runs the technical/tactical side of the response.

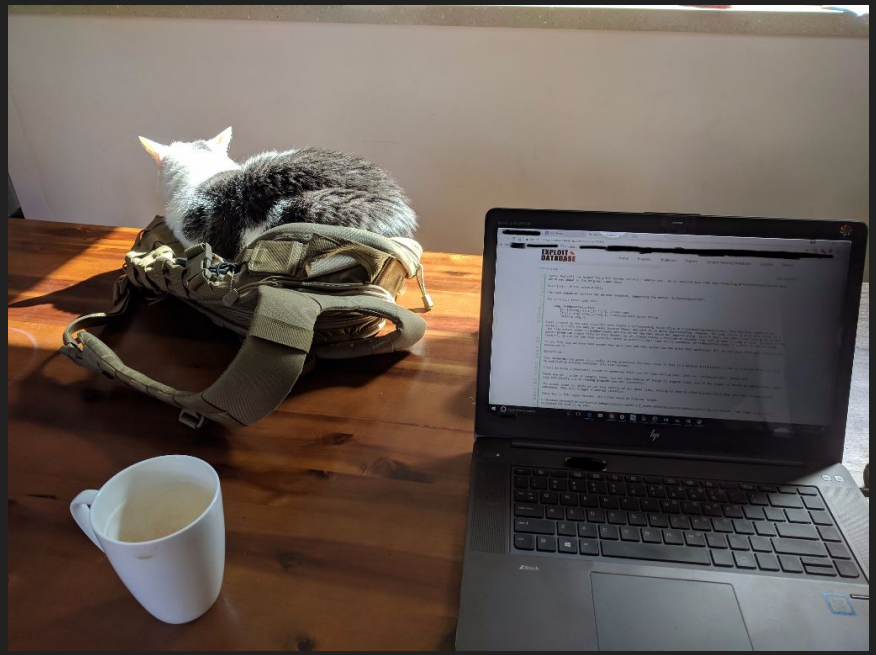
They select team members, assign tasks, and coordinate resources for the technical teams who perform the analysis and eventual remediation.

One additional part of the role is to ensure that all hosts/artifacts/indicators/findings/plans are documented and consistent.

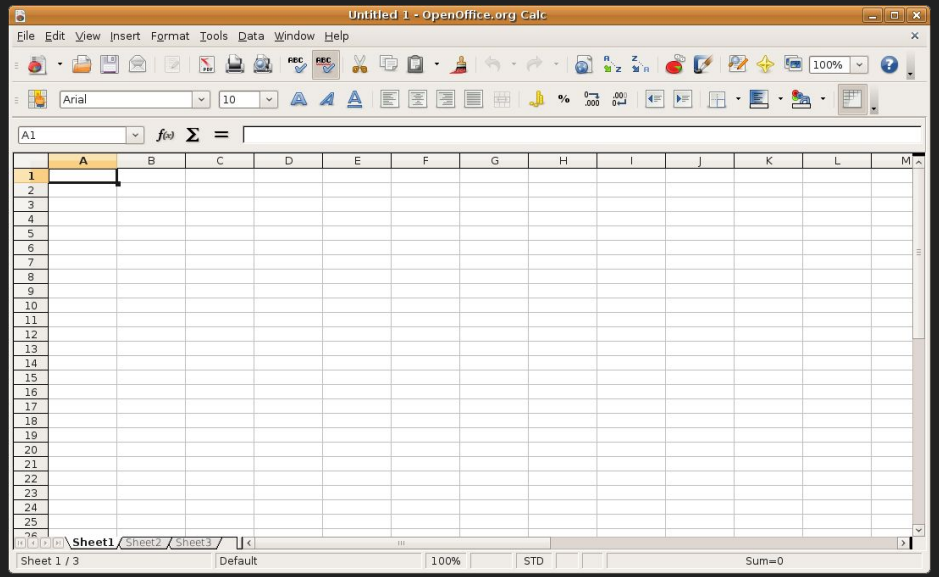
Like the IM/IC, they do not get to **do** the analysis itself.

Role Breakdown - Ops Lead(s)

[what you think ops lead is]



[what it actually is]

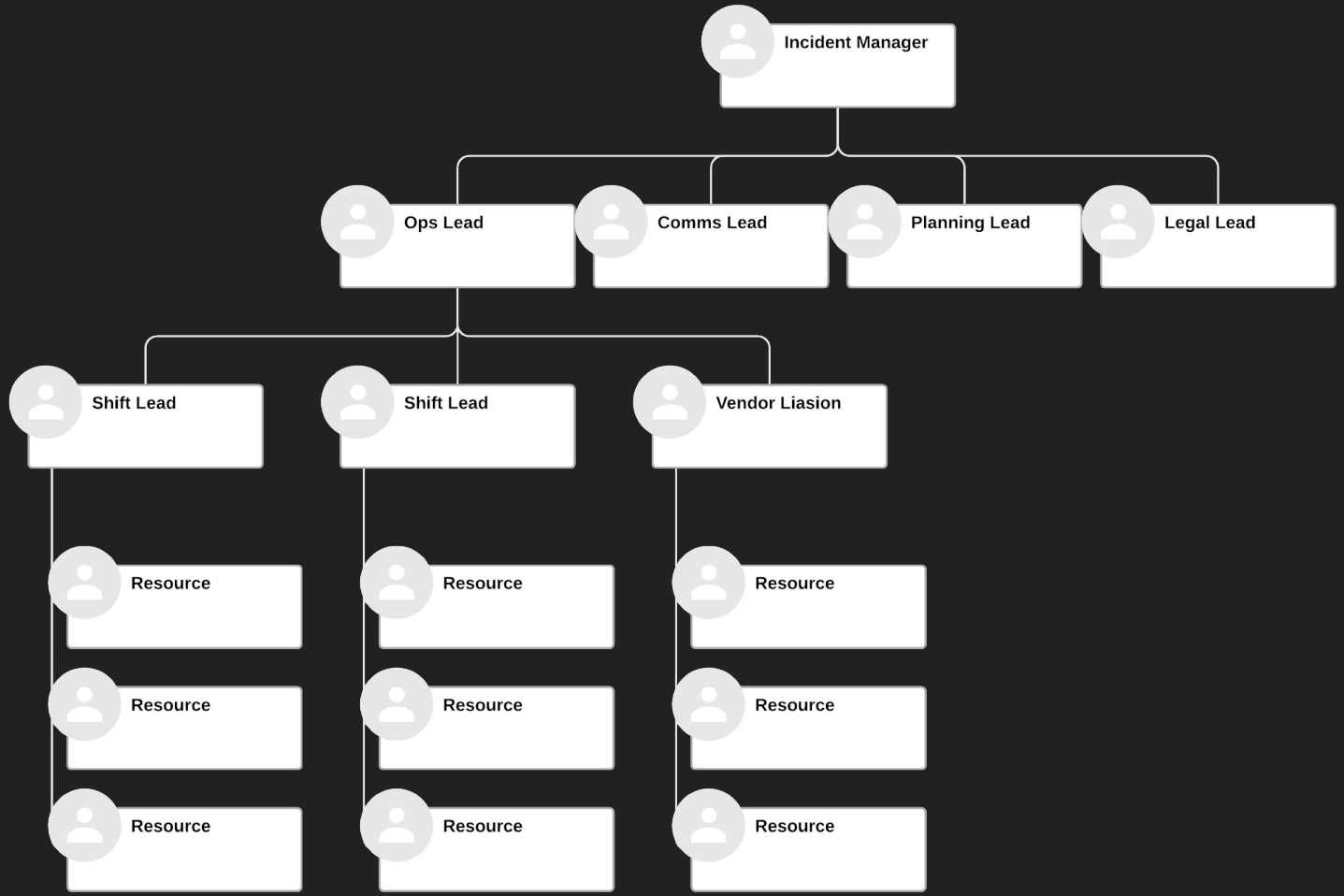


Role Breakdown - Comms Lead

The Comms Lead ensures that all stakeholders are informed - internal and external.

This will involve everything from drafting the Executive Updates, to writing tweets and blog posts (as required)

They answer the questions, and take input from external parties.


Incident Manager
Ops Lead
Comms Lead
Planning Lead
Legal Lead
Shift Lead
Shift Lead
Vendor Liasion
Resource
Resource
Resource
Resource
Resource
Resource
Resource
Resource
Resource

Incident Wrap-up

Blameless post mortems are invaluable for focusing the lessons learnt from the incident:

- What Went Well?
- What Failed?
- Where Did You Get Lucky?
- How Can You Prevent/Detect This In Future?

Other things to reflect on:

- How did the process work well?
- How could it be improved?
- How comfortable was everyone in their roles?

(*) If the incident was an exercise, make sure that at the other side is involved in the post mortem process, or produces one of their own.

Every Incident Is Unique

Treat every case as a unique challenge.

Have a well practiced plan, and stick to it.

Playbooks, Process, Practice.

Practical Advice

Eat, Sleep, Take Breaks

Keep watch for "well intentioned" helpers - the IT support team that turn the infected server off, the amateur sleuth who decides to look at attacker controlled domains and tipping them off, etc.

Plan remediation as you go - part of the Ops Lead role is to maintain registers of affected machines, accounts, cloud services, binaries, domains, ip's. As the incident proceeds ensure that all the required contacts and cleanup procedures are cross-linked.

DON'T PANIC

Thanks!

@bryannolen on Twitter

https://keybase.io/bryannolen