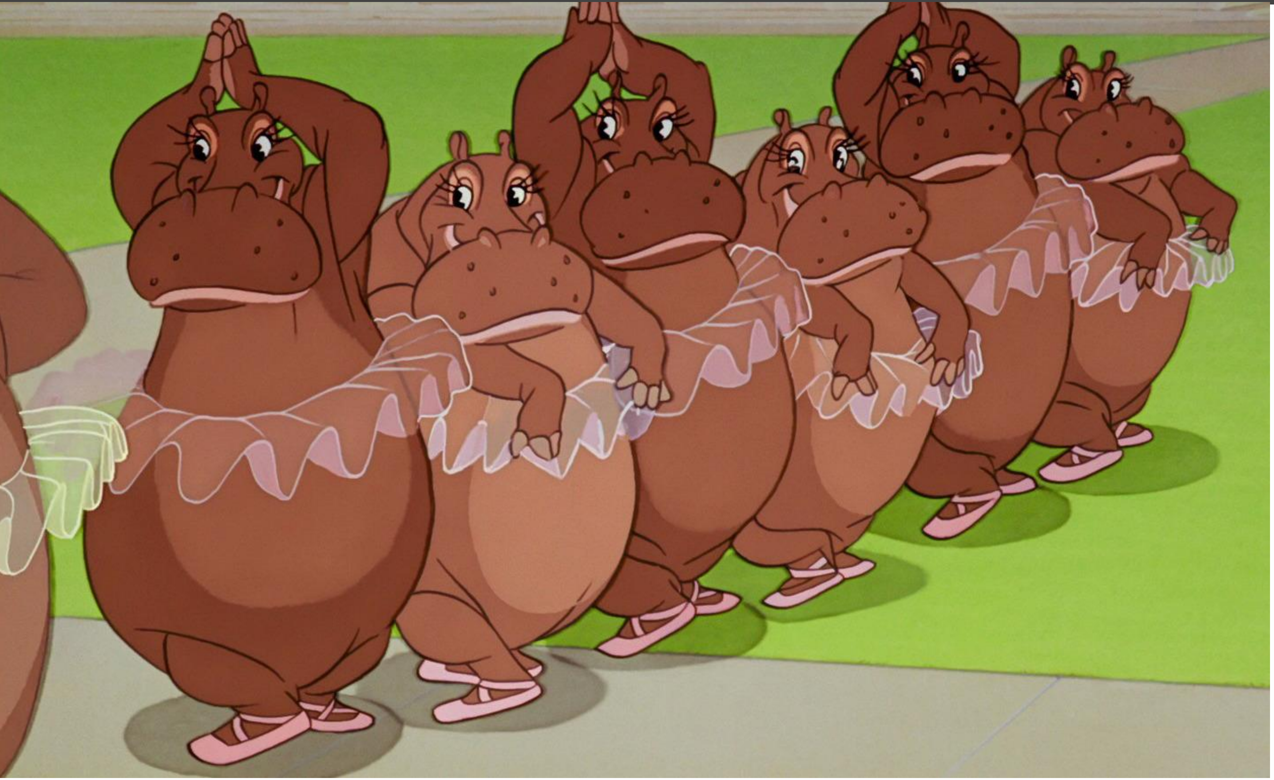
The Remediation Ballet



Matt Linton
Chaos Specialist
Google

What is the remediation ballet?

☠Incident Response is like choreography

☠Keep all the pieces moving

☠In sync, perfect timing

☠Incident Response *supports* Remediation

Your goal

☠Every entity has different drivers & goals.

☠One IR Goal: To become whole & functional again

☠Stronger, better if possible

☠Reputational damage minimized

☠This is why we have Incident Response

There’s incidents, and there’s *incidents*.

There’s incidents, and there’s *incidents*.

- ☠Every day incidents can, should be playbooked
- ☠Today let’s call those “Mishaps”
- ☠Larger, more complicated things are incidents.
    - Locky on a desktop? Mishap.
    - Phished account? Mishap.
    - APT Phished a domain admin last month? *Incident*.
- ☠Listen to the pit in your stomach

An everyday, ordinary incident

- ☠Car into hydrant
- ☠People hurt
- ☠Transformer flooded
- ☠Electric short
- ☠Accident investigation

Where to start?

☠Shut off water first?
☠Shut off power first?
☠Help occupants first?

☠Crispy water employee
☠Power guy hit by truck
☠Fried, soggy responders

Control traffic, cut water up street, shut off power, help occupants, investigate accident

What this has to do with “Cyber” IR

- ☠There are lots of things needing done
- ☠Each depends on something else in parallel
- ☠Going in the wrong order may make things worse

What this has to do with “Cyber” IR

☠If only someone had solved this problem before!

ICS: The Incident Command System

☠Developed by disaster experts

☠A flexible framework for doing this kind of thing

☠**3 C’s:** Command, Control, Communications

Example: Communications

- Hurricane Katrina Response, NOLA
- Simple task: Find survivors, relay GPS coordinates
- N 30°01’15” x W 90°01’26”

- Lat: 30.0209844 Long: -90.0239323

- NATO UTM z15, E 787039.4,   N 3324842.4

ICS: The Incident Command System

☠“Incident Commander” (incident Coordinator) is in charge

- They appoint “Operations Lead”
- Can appt “Communications Lead”, “Planning Lead”
- Can make up positions as needed, too

☠IC: **Strategic** vision & coordinates the response

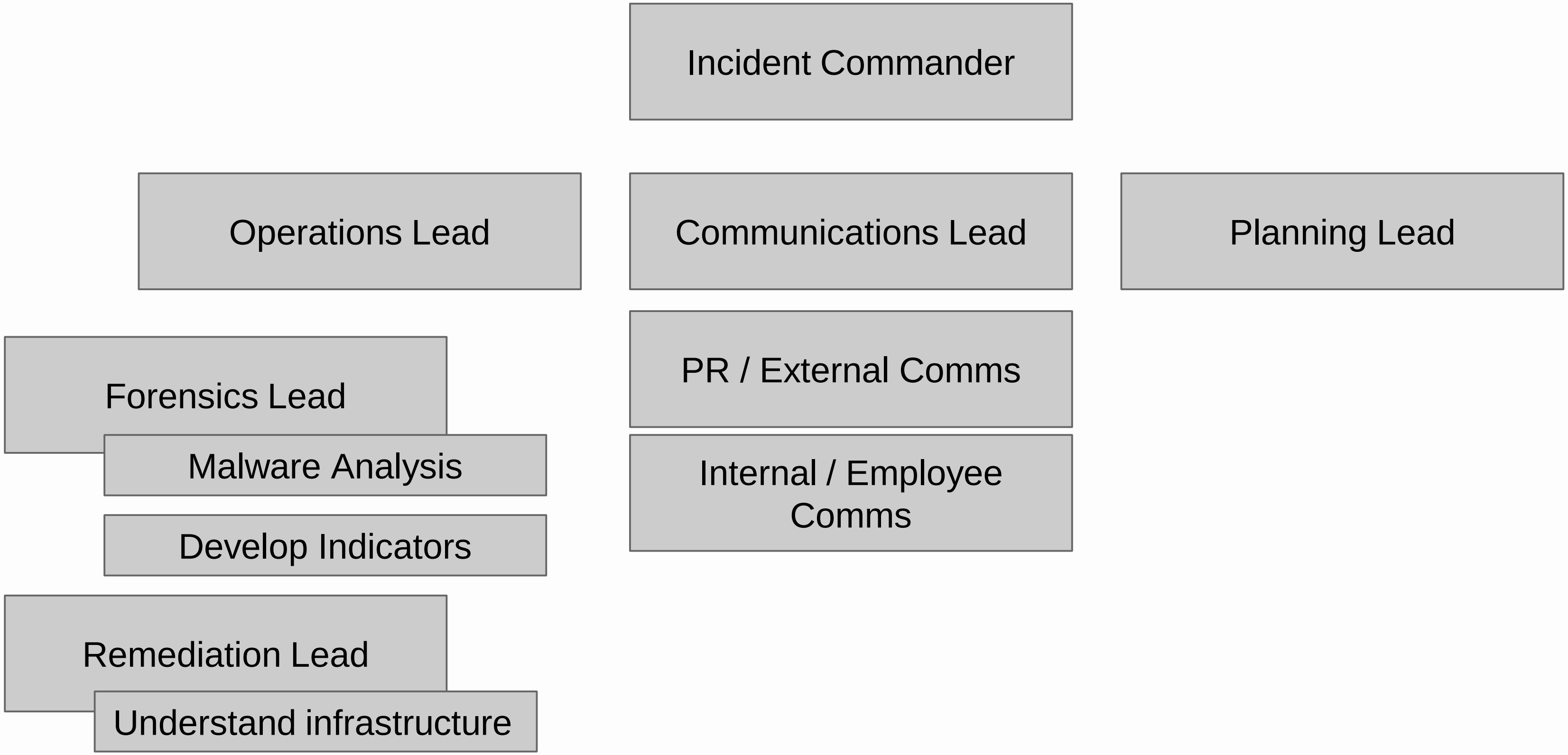
☠Ops: **Tactical** approach to broad objectives

ICS: The Incident Command System

☠Incident Commander

- Will consult with management / stakeholders on decisions
- But must be **empowered** to make calls on the spot
- Builds a circle of advisors (Ops Lead, Lead techs)

ICS: The Incident Command System



Incident Commander

Operations Lead

Communications Lead

Planning Lead

Forensics Lead

Malware Analysis

Develop Indicators

Remediation Lead

Understand infrastructure

PR / External Comms

Internal / Employee Comms

ICS: The Incident Command System

☠Chain of command

☠Non-ambiguous

☠Everything is explicit

☠Roles are defined, people know their job

☠Handover is NOT AUTOMATIC

WARNING:

☠The framework is for managing the incident

☠Don’t let it become “heavy”

☠Or too light

☠Manage to the degree warranted by the incident

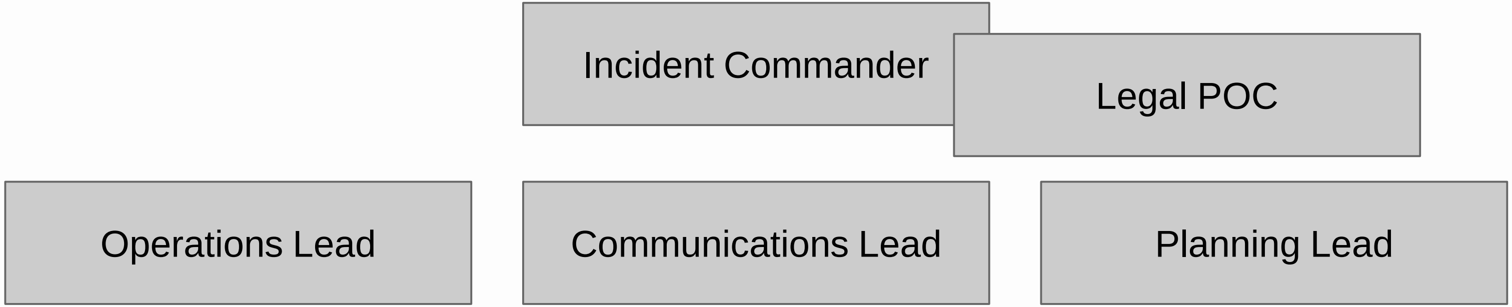
Let’s do this!

- ☠️Hey, why is the domain controller full of RAR files?

Let’s do this!

- ☠ Initial reaction
  - Confirm. Is this true?
  - Declare incident, assign operations lead
- ☠ Establish the “war room”
  - Decide where/how to meet & communicate
    - Email? IRC? Phone bridge? Videoconference?
    - In person always great if possible
- ☠ Take 5 minutes to collect your thoughts

Let’s do this!



Incident Commander

Legal POC

Operations Lead

Communications Lead

Planning Lead

Tools/Capabilities to investigate?

Qualified staff?

Enough staff?

Do we have access? Who does?

Who knows?

Brief everyone on confidentiality aspects?

Prepare summary if needed for lawyers?

Start controlling the information spread

What funding might we need?

How quickly can we hire surge help if needed?

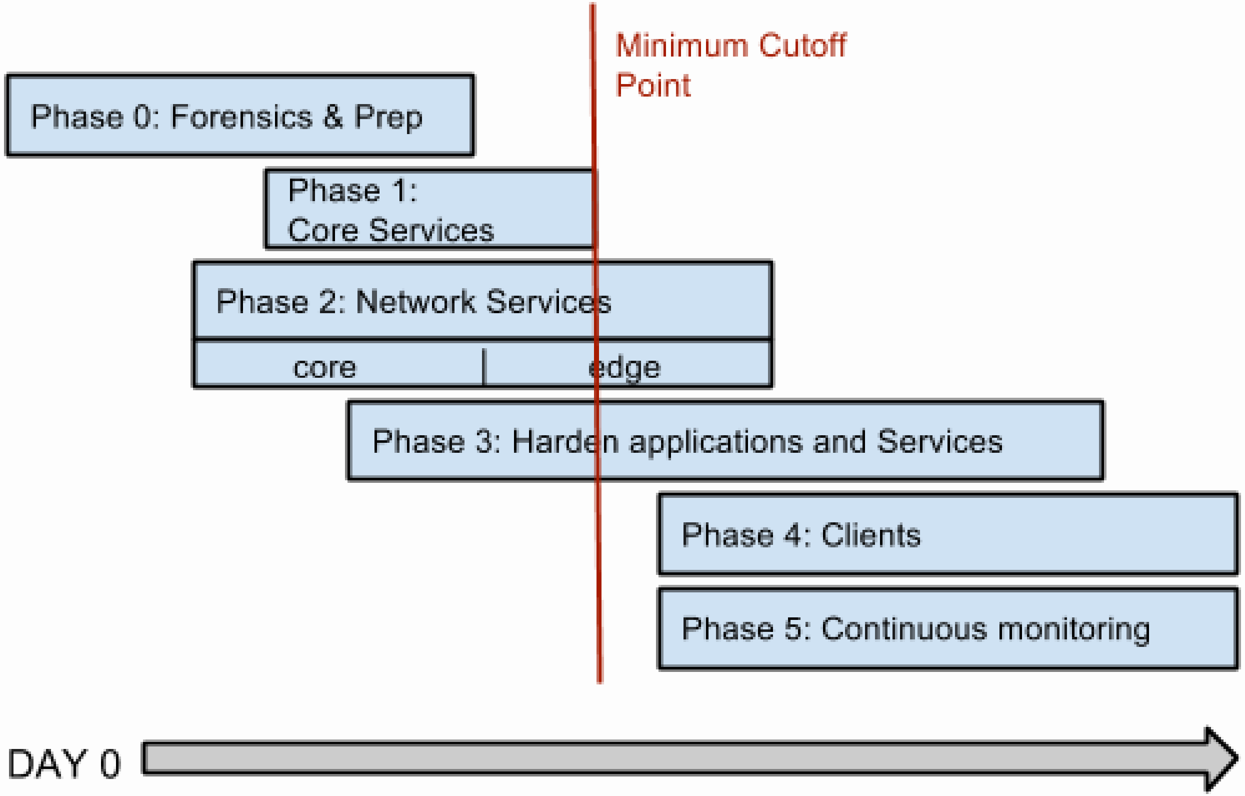
Engage with CFO/Finance for surge needs?

Let’s do this! [Phase 0]

☠Lets go through a major incident. Assumptions:

- We are thoroughly pwned
- We want to completely clean up with high certainty
- Org can tolerate some downtime but prefers as little as possible
- VIP’s, some branches need to be working sooner than others

A rough sketch of a large incident response


Minimum Cutoff Point
Phase 0: Forensics & Prep
Phase 1: Core Services
Phase 2: Network Services
core
edge
Phase 3: Harden applications and Services
Phase 4: Clients
Phase 5: Continuous monitoring
DAY 0

Let’s do this! [Phase 0]

☠PHASE 0 - Forensics/Investigation

☠IC Strategic need to determine:

- Scope/extent of the compromise
- Capabilities of malware/implants/attacker
- Obligations, notification deadlines, etc
- Likely business impact

☠Ops focuses on finding not fixing (in this phase)

Let’s do this! [Phase 0]

☠Scope

- One system? A few? Trusted or untrusted?
- Opportunistic or Targeted?
- User creds leaked? What privs did they have?
- Remote access methods?
- What/When/How
    - Resist temptation to answer “Who” and “Why”

Let’s do this! [Phase 0]

☠Capabilities

- C2 Implant?
- How does the attacker hide? Where?
- More than one?
- Webshells?
- How much of your infra is “theirs” now?
- Accounts too!

Let’s do this! [Phase 0]

- ☠Obligations
  - Customer notification deadlines (within X days…)
  - Statutory? Contractural? What starts the counter?
  - You’ll need your favorite Lawyer here…
- ☠If you determine notification obligations, you need a planning lead
  - A PM to track schedule

Let’s do this! [Phase 0]

☠Impact

- What’s the impact of leaving the malware running while you study it?
- Study the attacker?
- What’s the impact of killing the access/malware?
  - Kill too late, you’ve lost your data
  - **Kill too early, you’ve tipped off the attacker**

A word on opportunity

- ☠Opportunity time
- ☠During cleanup/remediation we can harden too
  - IC + PL: What failures caused/contributed to this?
  - What missing controls can be speedily implemented?
  - Find the security-aware sysadmins and ask:
    - “Where’s your list of things you’ve been asking them to do forever and they won’t?”
    - **“Which protections would have had an impact here?”**

Phase 1 - Core Services

☠ C/C/R (Clear, Clean or Rebuild) the core services

- If rebuilding, rebuild in an air-gapped place & stage
- If you just need a clean config, prep it air-gapped on staging gear
- LDAP/AD servers, Mailserver
- Might be a good time for binary whitelisting/blacklisting

Phase 1 - Core Services

☠ Mailserver

- If users got phished / viruses, are they still latent in mailboxes not yet checked? Search + Quarantine!

☠ File Servers

- Checksum all malware/artifacts
- Recurse-checksum fileservers & Hunt

☠ Credentials

- User password changes; Privilege audits.
- Service accounts and SSH keys!

Phase 1 - Core Services

☠ Adjust the defensive posture

- Consider a bulkheaded design for an improved network
- Control RDP/VNC/SSH with 2FA proxies, GPO, Puppet+iptables, etc

If only we'd built it with 6,001 hulls!
When will humanity learn!?

Phase 2 - Network Services

☠“Core” vs “Edge”

☠Clear/Clean/Rebuild + Harden:

- Router/firewalls
- Transit network gear
- Edge network gear

☠Hey, have you considered VLANs yet?

Aside

☠Network core is clean/fixed/new

☠Critical services are clean/fixed/new

☠Now is when I like to do the sudden-death cutover

☠Nothing touches the new network until it’s clean!

Phase 3 - Apps & Services

☠ C/C/R + Harden:

- Wikis, repos, CAD, etc
- Here’s a good time to look into service accounts / trust in app land
- Internal apps (payroll, salesforce, etc)
- Check API token use/theft too!

Phase 4 - Clients & General IT

☠️C/C/R + Harden:

- Desktops, Laptops (VIP’s first, etc)
- Anything with a filesystem
- Anything with a network connection

Phase 4 - Clients & General IT

- ☠ Forget something?

Phase 5 - Lay traps & Monitor

☠ Attackers will come back

- Honeypot where a critical server once was?
- “Retire” compromised usernames, detect failed logins

Tips, Tricks, Traps & Tacts

☠Many people will dual-role...

☠Never combine IC & Ops Lead!

- IC is stepping back, big picture
- OL is leaning in, focus on details
- Very hard to cycle between

Tips, Tricks, Traps & Tacts

☠ Some “Facts of Life” for responders

- Your stamina - 12 hrs/day max. You’ll burn out.
- Span of control: ~ 7-ish.
- “Point of Diminishing returns” on responder effort

☠ Consider these at all times

- Calendar yourself time every X hours
- “How are things going? Do I need more help/resources?
- “Will I need to hand over?”

Tips, Tricks, Traps & Tacts

☠ How to tell if you’re overwhelmed

- I’m annoyed at my Ops Lead
- “I don’t have time for this!”

☠ Balance debate with action

- Limited debate necessary for good decision making
- But avoid debate paralysis

Tips, Tricks, Traps & Tacts

☠ Handovers

- Direct from role-to-role (eg, IC to IC, OL to OL)
- Explicit (Next cycle plans were X, Y, Z)
- Good notes are key
- “What would you be doing in the next 12 hours if you weren’t handing over to me?”

Tips, Tricks, Traps & Tacts

☠ Control squirrels / freelancers

Tips, Tricks, Traps & Tacts

☠ Feeding your staff

- Food comes to them or they will go to the food
- Disorganized, ad-hoc
- Plan to provide this

Tips, Tricks, Traps & Tacts

☠Control the “Hero burnout effect” on staff

…. Including yourself!

Conclusion

- ☠Studies show* that engaging both the logical and artistic centers of the brain can help with information retention

With that in mind…..

** I made this up. But I think it’s true.*

PS - Google IR is hiring!