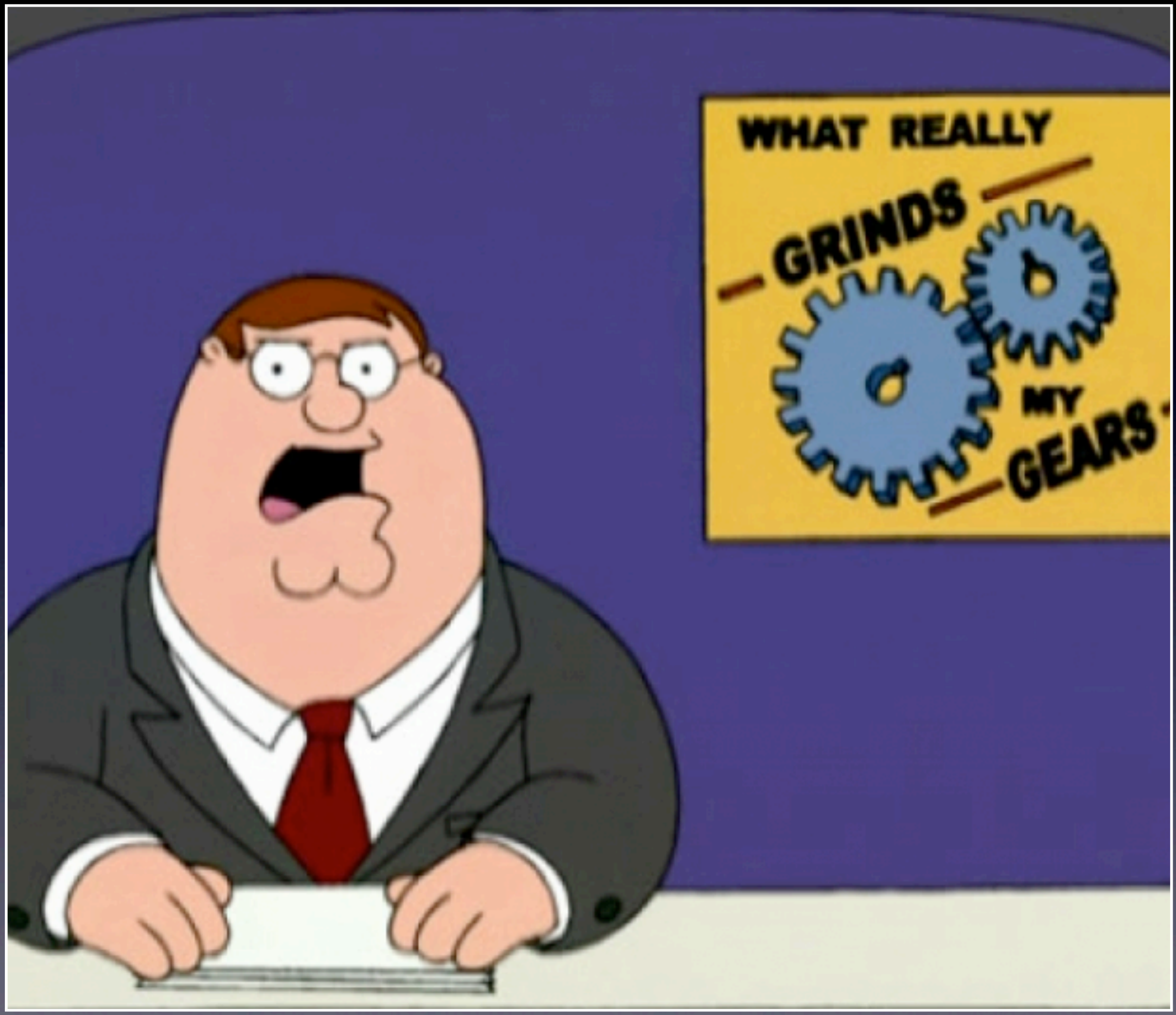
Third-Party Incident Communication

Julien Goodwin
jgoodwin@studio442.com.au


WHAT REALLY
GRINDS
MY
GEARS

Who am I?

- Make it clear who you represent
  - Remember to give detail if you've changed company name or may be best known by something else
- If you're an outsourced service give details of both sides

Example Technical Information

- IP - Source & destination subnet(s)
  - Consider including traceroutes if issue looks to be at IP level
- BGP - AS number, peering IP(s)
- WWW, e-mail - domain names
- Recursive DNS servers
- Any traffic manipulating devices in path?
  - (Proxies, SSL inspection, etc.)

Who are they?

- Make it clear who you're contacting so the recipient doesn't start going on a wild goose chase for something unrelated

Example Information

- As on “who am I”, plus:
  - “Provider of service X for domain Y”
  - “Apparent transit/DNS provider for Y”
  - Circuit ID’s, reverse DNS entries

What's the problem?

- Make it clear what the actual problem is
- Not just what you've isolated it to
- Remember that many troubleshooting steps give false positives over the internet
  - eg, traceroute

Why do they care?

- Being able to show impact to the third party or their customers helps get them to care