



Incident management insights

By

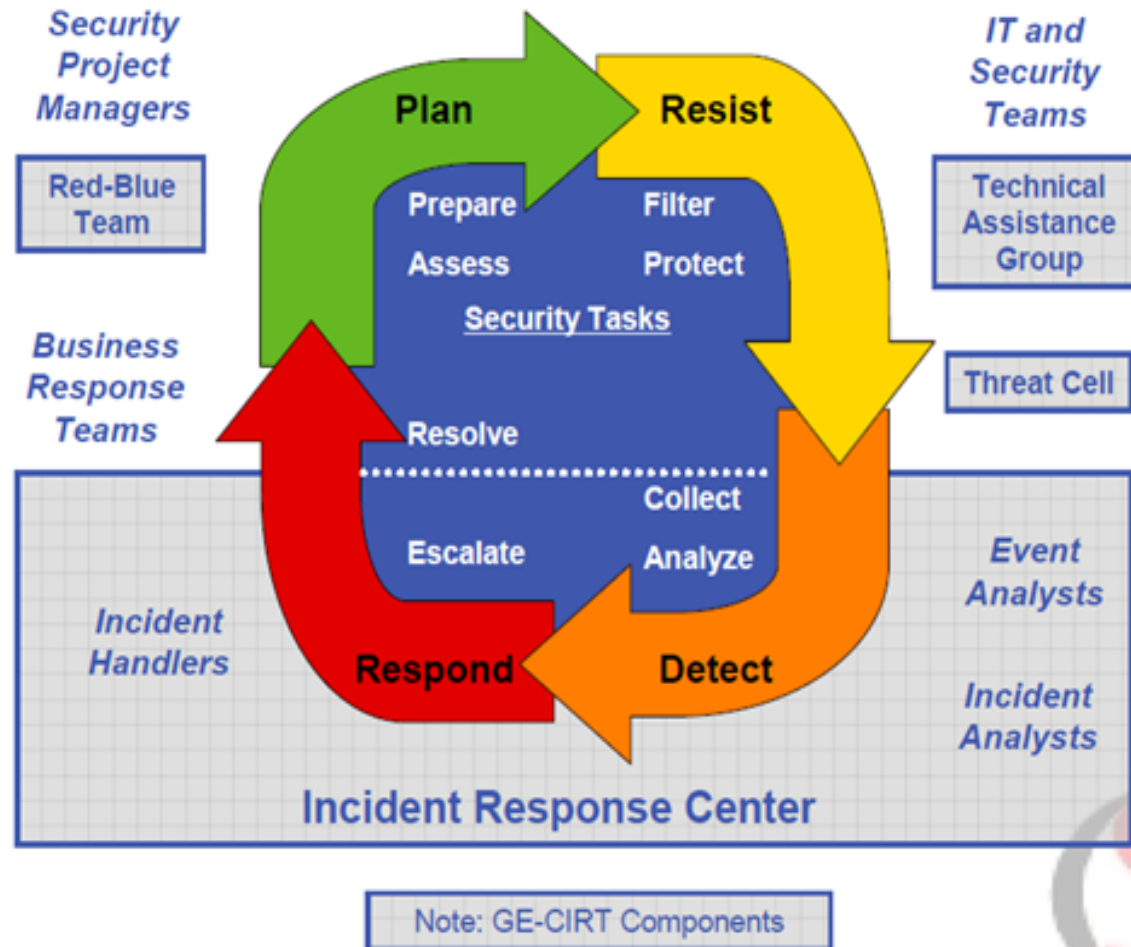
Hariprasad Chede

CISSP, CGEIT, CISM, CFE, C-CISO, CIPR

CISO – National Bank of Fujairah

Incident management is not a linear process; it's a cycle that consists of a preparation phase, an incident detection phase and a phase of incident containment, mitigation and recovery. The final phase consists of drawing lessons from the incident in order to improve the process and prepare for future incidents.

What should not be done...



1. Poor Planning

To have a perfect strategy

2. Resolute Resistance

Process when the resistance mechanisms fails to block attacks

3. Dramatic Detection

Detected but no sure how to resolve them.

4. Ravenous Response

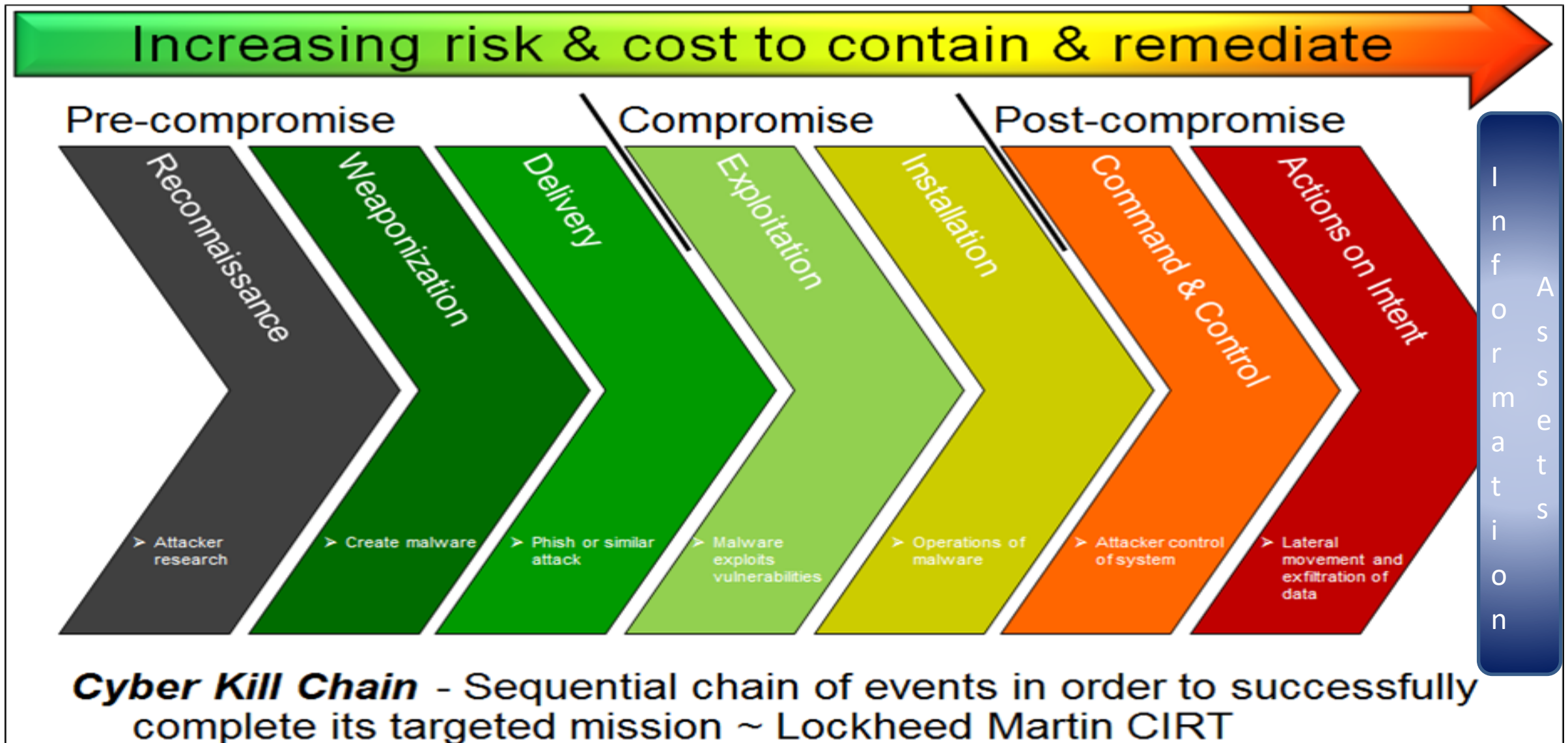
Rate of incidents > the responds

Source: Richard Bejtlich, *CIRT-Level Response to Advanced Persistent Threat*

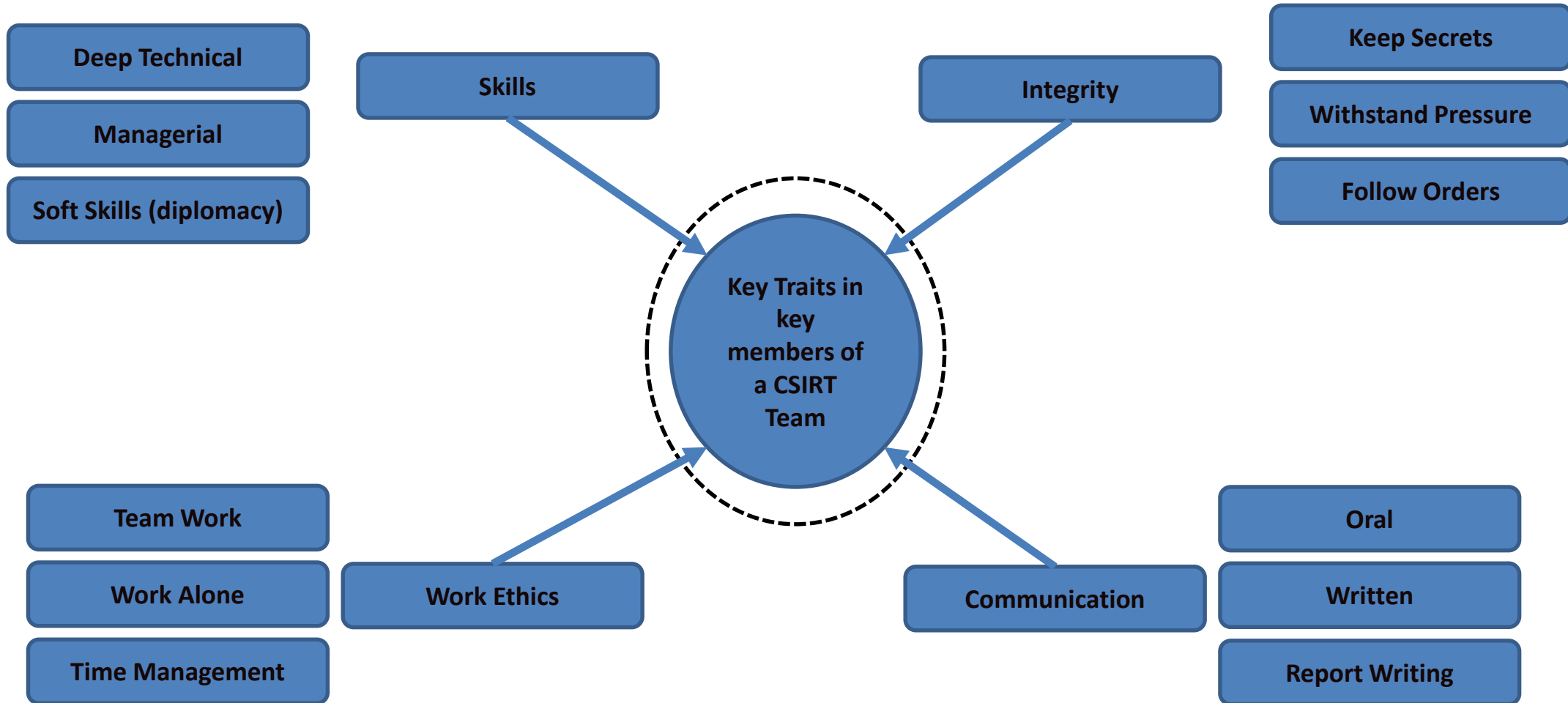
Incident Handling – Practical Tips...



Collaboration !!



BUILDING THE TEAM



Trust Your Technical Leads...

- **Guys on the ground will be best placed to respond**
- **Should be capable to take independent action may breach protocols, SLA's etc.**
- **Countermanding their actions without superior knowledge**
- **Do not second guess technical decisions.**
- **Ask for options if necessary; be prepared to offer them but receive none in reply.**



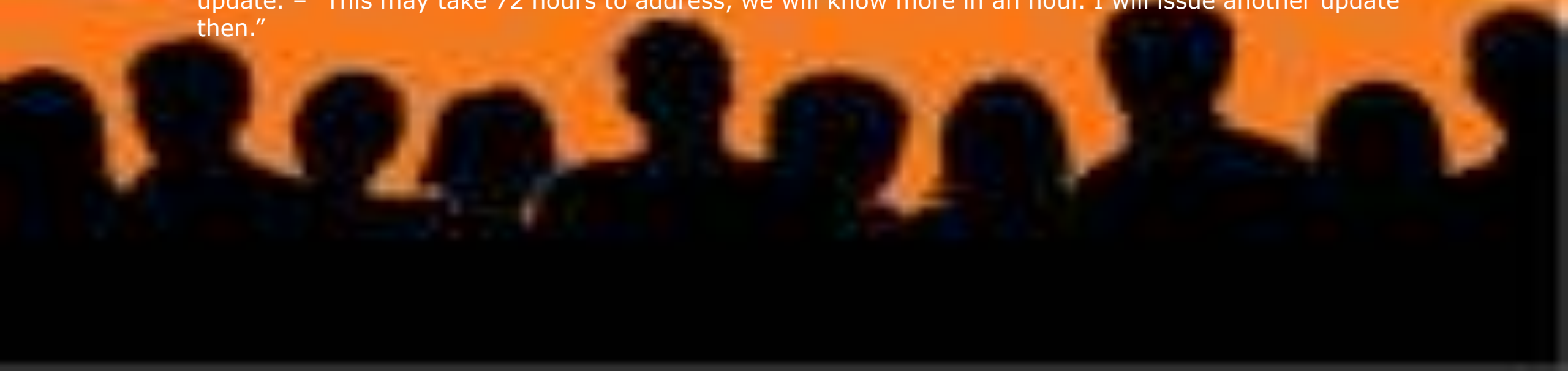
The Definition of an "Acceptable Loss"



- Exercise judgment and say to yourself "this decision is above my grade"
- Have two-way communication with the business
- Have the argument with yourself if necessary beforehand to prepare better counter arguments.
- Being aggressive or derisive will not move the situation forward

Do not assume your audience is incompetent or an expert

- **Flow of information up and down the chain of command is key.**
- **Further you go up the chain, likely less technical the audience**
- **Communications be as succinct as possible**
 - Explain the problem – “There is a problem with the server which is affecting customer ABC.”
 - Explain what you are doing to investigate/correct the issue – “We are currently on the phone to the vendor.”
 - Offer what the next step might be – “They may need to issue a patch.”
 - Suggest a timeframe for a resolution or at the very least the next update. Stick to the timetable for the update. – “This may take 72 hours to address, we will know more in an hour. I will issue another update then.”

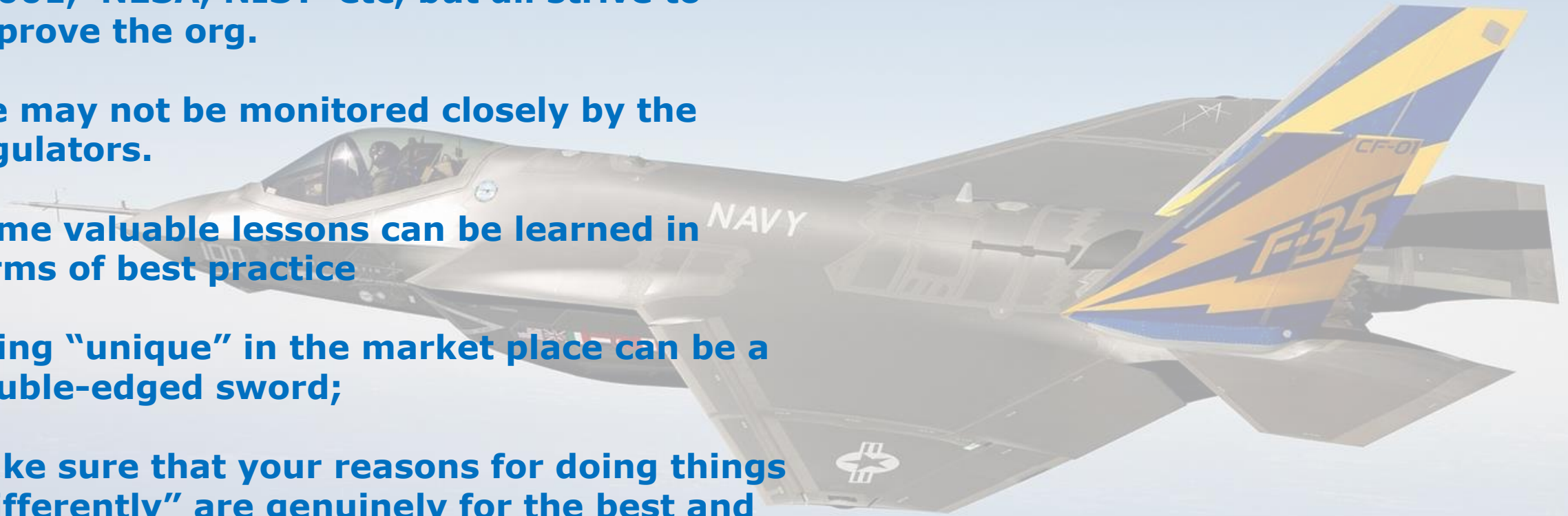


Have a Plan - B

- If your key monitoring system is dependent on your production system in any way, then you need to have a plan B in the event of failure
- Good practice to have a "battle box" of basic equipment available in the event of an emergency.
- Bare-essential items such as patch leads, serial cables, an old (but reliable) laptop with basic system management tools, screwdrivers, fuses, and possibly items such as basic switches or routers.

Sometimes there is a reason why everyone else does it that way...

- Might have bored with the standards like ISO 27001, NESA, NIST etc, but all strive to improve the org.
- We may not be monitored closely by the regulators.
- Some valuable lessons can be learned in terms of best practice
- Being “unique” in the market place can be a double-edged sword;
- Make sure that your reasons for doing things “differently” are genuinely for the best and not to the ultimate determinant of the business.



Access to up-to-date documentation is mandatory



- Documentation is one of those jobs that no one ever wants to do;
- Being able to access knowledge like “which switch port the internet router is connected” immediately is the kind of thing which may save the situation.
- Discipline in maintaining documentation is critical
- Have a hard copy or an electronic copy *somewhere* which can be independently powered and accessed.

There is always a worse, worst-case scenario

- **It's clear that information security risk management cannot foresee every eventuality**
- **Even exploring the "worst case scenario" can be helpful.**



Examples:-

- **What would we do if the power was to fail at the primary data center during a scheduled outage at the DR site?**
- **What would we do if we found the Customer Oracle Database was corrupt whilst all the DBA's had food poisoning?**
- **What would we do if the building next door was to catch fire and the emergency services prevented access to our building?"**
- **How to get the data when all critical servers got wiped off...**

How many of us have an emergency kit @
Home?????

Hariprasad Chede

All photos have been taken from Google search