PATCHING STUPIDITY

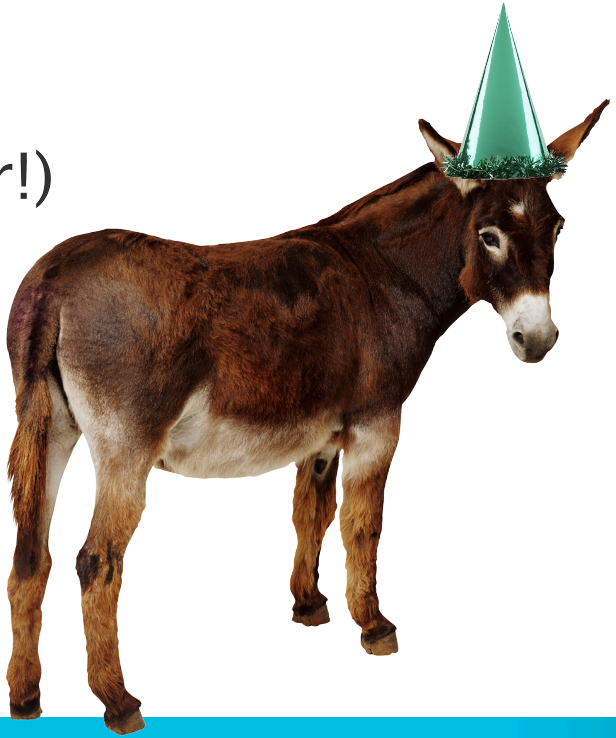
Jack Jones
CXOWARE

Session ID: MASH-T19

Session Classification: General Interest

What we'll cover…

- What do we mean by "stupidity" anyway?
- What does "stupidity" look like?
- Understanding what drives "stupid" behavior
- The assessment process
- Example results (Metrics that matter!)
- Sources of data
- Using the results
- Q&A



What do we mean by "stupidity"?

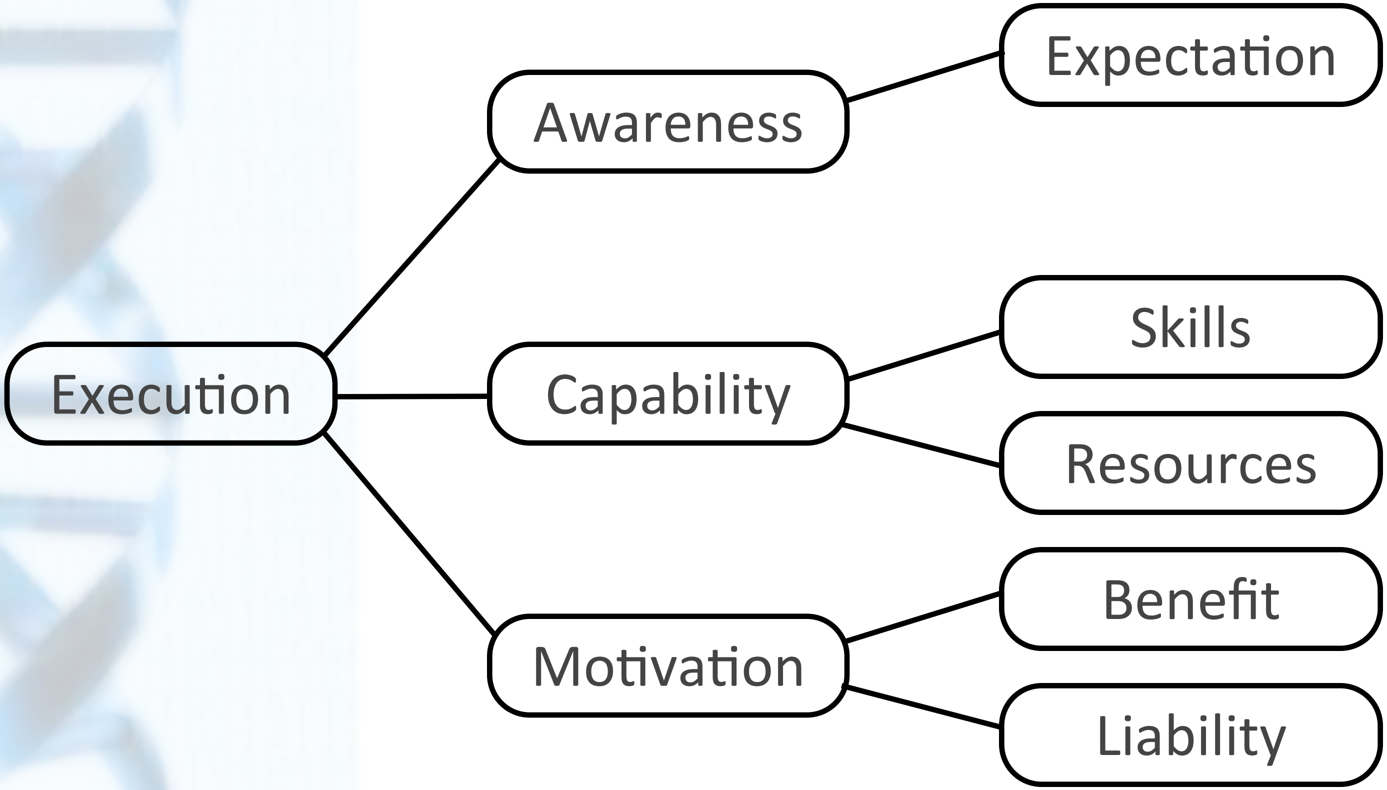
Decisions and actions contrary to
infosec policy and/or "common sense"

Before we can "fix" it...

... we have to understand what's driving it.

Hint -- it's (probably) an execution problem.

A framework for evaluating execution failures

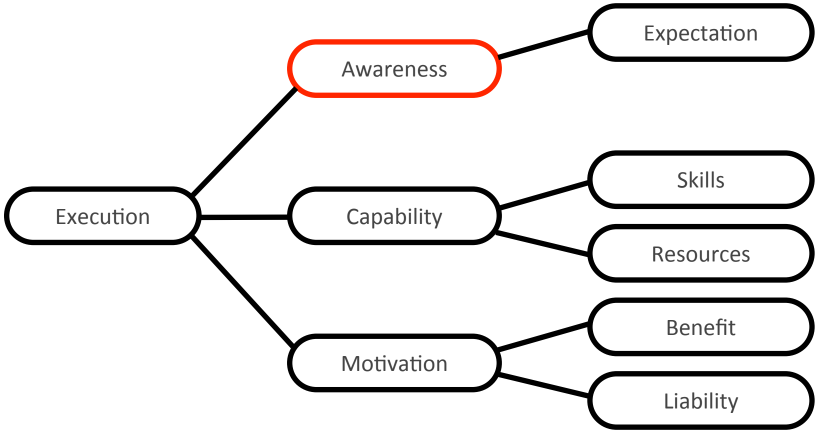


- Execution
  - Awareness
    - Expectation
  - Capability
    - Skills
    - Resources
  - Motivation
    - Benefit
    - Liability

Example execution failures for analysis...

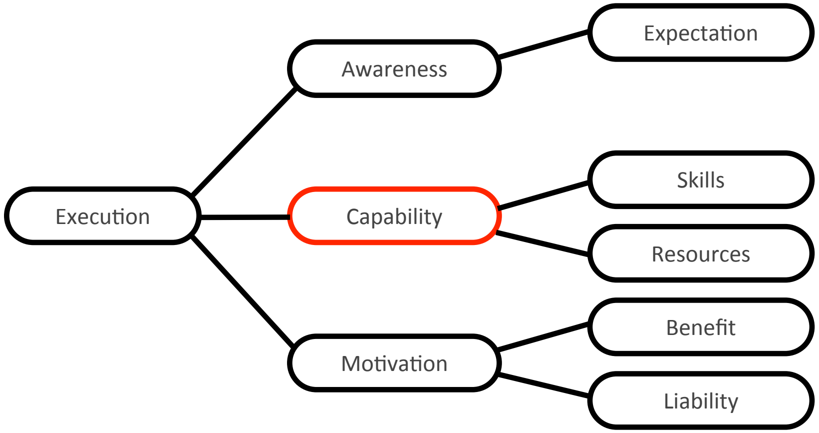
Missing patches
Sensitive information in public trash receptacle
Microsoft SQL Server SA account default blank password
CISCO device default password
Shared passwords
VNC server unauthenticated access (all pc's)
Unsupported LINUX operating system
Mountable NFS shares
Writing passwords on sticky notes
etc...

Example process...



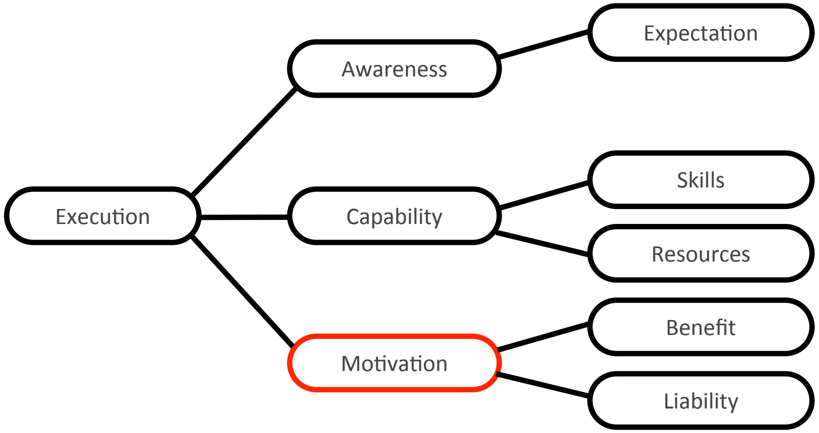
- **Line of questioning:**
  - Is there a documented and published expectation (e.g., policy) related to the issue?
  - Were those responsible for compliance aware of the expectation?
  - If not, then this is the likely cause in this instance. If they were aware, then...

Example process…



- **Line of questioning:**
  - Were those responsible, capable of complying? I.e., Did they have the necessary skills and resources?
  - If not, then this is the likely source of the problem. If they did have the necessary skills and resources…

Example process...

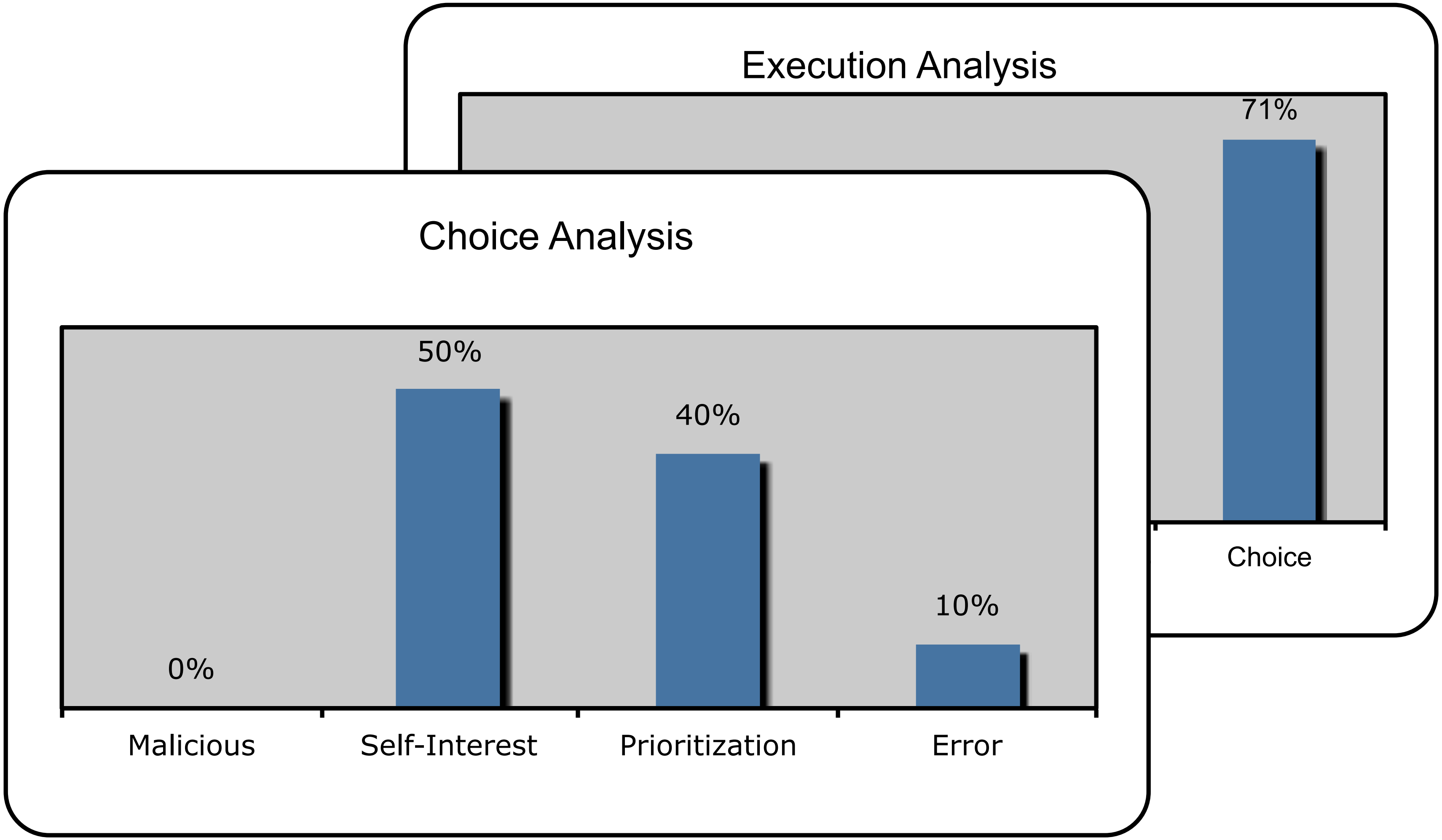


- **Line of questioning:**
  - If they were aware and capable, then a choice was made.
  - Was the motivation behind non-compliance a matter of maliciousness (an intent to cause harm)? If not...
  - Was the motivation a matter of personal self-interest (e.g., laziness)? If not...
  - Was the motivation a matter of choosing to prioritize compliance lower than other organization imperatives (e.g., budget or deadlines)?

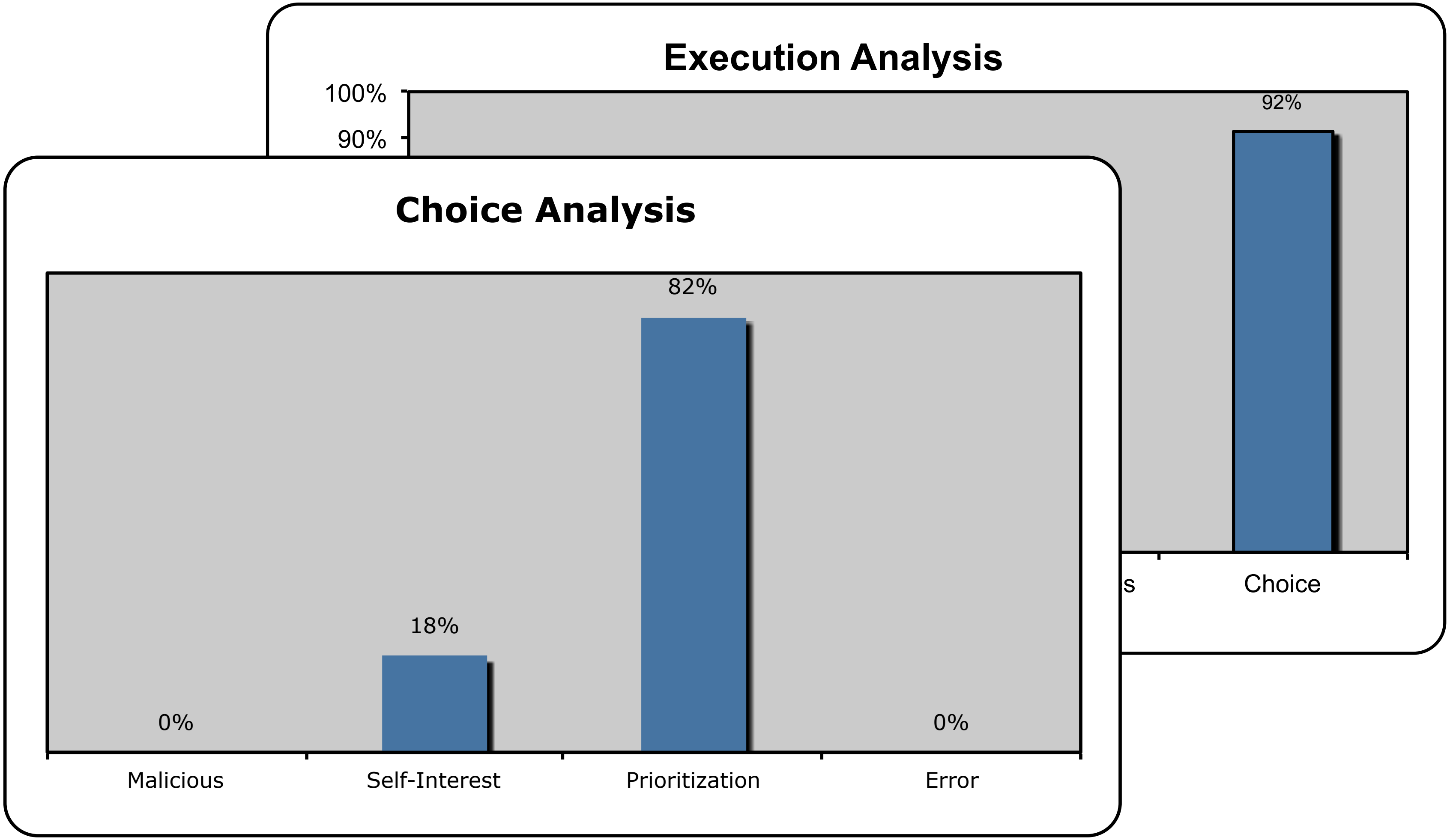
The process…

Simply follow this line of questioning for every instance of “stupidity”, and record the answers.

Example results



Example results



Sources of data...

- Audits
- Security testing
- Risk registers
- Incidents (and not just infosec)

What to do with the results

- Develop focused strategies to address the results, for example:
  - Focused awareness campaigns for trouble spots
  - Improved skills training and/or resource availability
  - Improved communications from executives regarding proper prioritization of infosec compliance
  - Improve methods for holding people accountable
- Integrate these questions in the incident response and investigation process, and for all audit findings
- Track improvement/changes in monthly metrics, or...
- Adjust the policy/expectations

Summary

- It’s difficult to fix something unless you know what’s causing the problem in the first place
- You can learn a LOT about an organization through this process
- Awareness may not be the most significant contributor to “stupidity” in your organization
- Effectively addressing the results of this assessment can have a significant impact on how much “stupidity” an organization experiences

Questions

For more information:

URL: www.cxoware.com
E-mail: info@CXOWARE.com
Phone: 866.936.0191