Ending Risk Management Groundhog Day

SESSION ID: GRC-R03

Jack Jones

President
CXOWARE, Inc.
@jonesFAIRiq

Agenda

- You know you’re in Groundhog Day when...
- How did we get here?
- Deming had it right
- The right questions
- Putting it to use

You know you're in Groundhog day when...

Dude... Again? Really?

You know you’re in Groundhog day when...

You see the same problems repeatedly

...even after you’ve “fixed” them

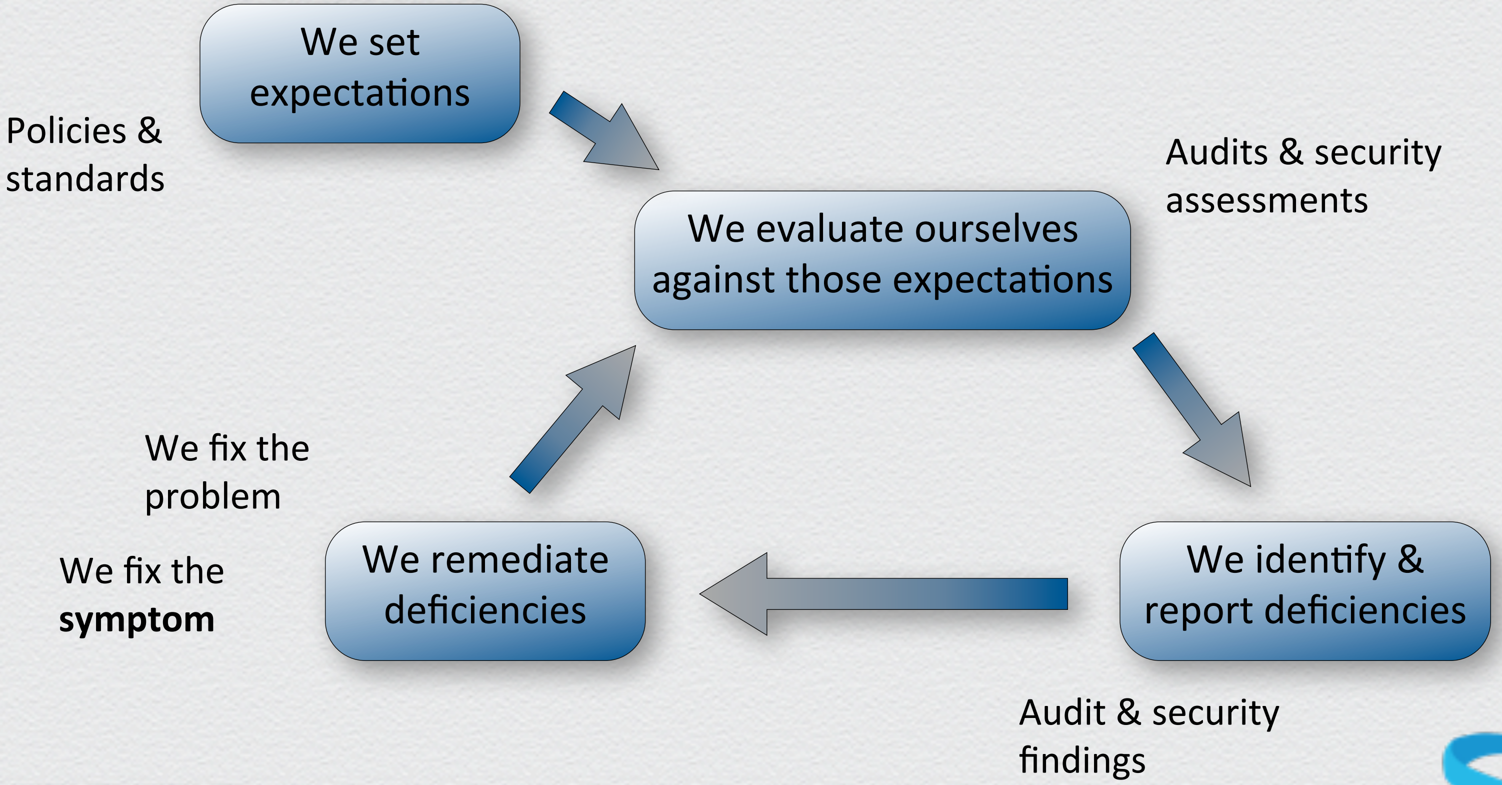
...multiple times

Common examples

- Access privileges not removed/changed
- Personnel writing passwords on sticky notes
- Change management processes not being followed
- Applications being developed with significant security deficiencies
- Patches not being applied in a timely manner
- People opening obviously questionable e-mail attachments...

How did we get here?

How did we get into GHD?



Policies & standards

We set expectations

We evaluate ourselves against those expectations

Audits & security assessments

We identify & report deficiencies

Audit & security findings

We remediate deficiencies

We fix the problem

We fix the **symptom**

How did we get into GHD?

What’s the primary reason why people

continue to make these mistakes where you work?

How did we get into GHD?

If you can’t answer that...

RSACONFERENCE2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Deming Had it Right

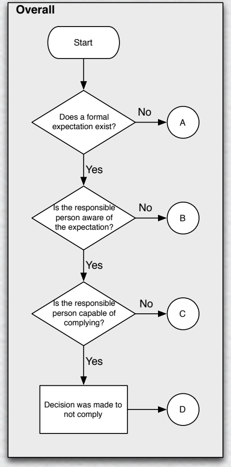
Deming Had it Right

“If you do not know how to ask the right question, you discover nothing.”

Edwards Deming

The right questions...

Flow chart



Overall

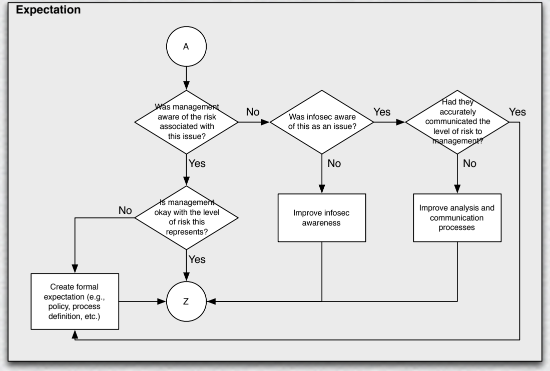
Start

Does a formal expectation exist? No → A; Yes

Is the responsible person aware of the expectation? No → B; Yes

Is the responsible person capable of complying? No → C; Yes

Decision was made to not comply → D



Expectation

A

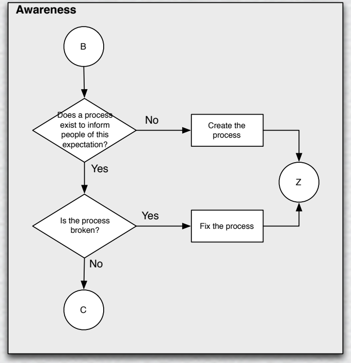
Was management aware of the risk associated with this issue? No → Was infosec aware of this as an issue? Yes → Had they accurately communicated the level of risk to management? Yes

Yes → Is management okay with the level of risk this represents? No → Create formal expectation (e.g., policy, process definition, etc.); Yes → Z

Was infosec aware of this as an issue? No → Improve infosec awareness

Had they accurately communicated the level of risk to management? No → Improve analysis and communication processes

Z



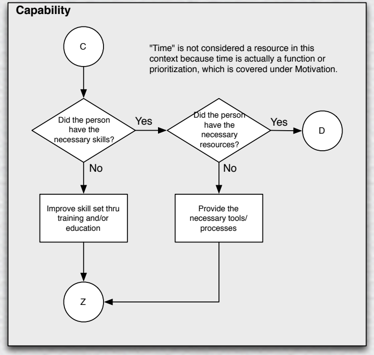
Awareness

B

Does a process exist to inform people of this expectation? No → Create the process → Z; Yes

Is the process broken? Yes → Fix the process → Z; No

C



Capability

C

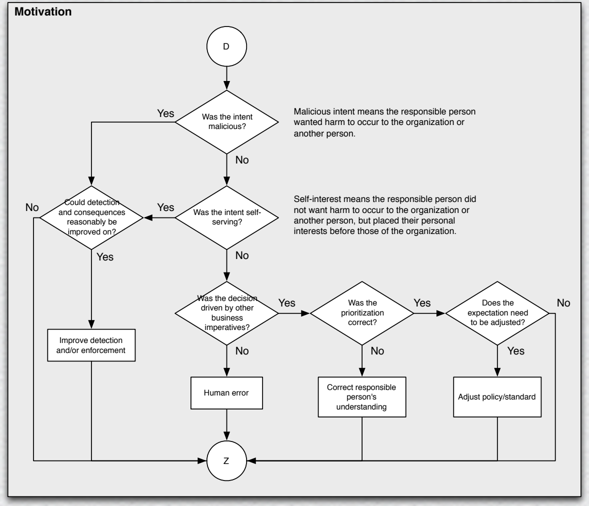
"Time" is not considered a resource in this context because time is actually a function or prioritization, which is covered under Motivation.

Did the person have the necessary skills? Yes → Did the person have the necessary resources? Yes → D

No → Improve skill set thru training and/or education

No → Provide the necessary tools/ processes

Z



Motivation

D

Was the intent malicious? Yes; No

Malicious intent means the responsible person wanted harm to occur to the organization or another person.

Was the intent self-serving? Yes; No

Self-interest means the responsible person did not want harm to occur to the organization or another person, but placed their personal interests before those of the organization.

Could detection and consequences reasonably be improved on? No; Yes → Improve detection and/or enforcement

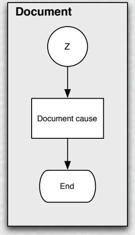
Was the decision driven by other business imperatives? Yes → Was the prioritization correct? Yes → Does the expectation need to be adjusted? No

Was the decision driven by other business imperatives? No → Human error

Was the prioritization correct? No → Correct responsible person's understanding

Does the expectation need to be adjusted? Yes → Adjust policy/standard

Z



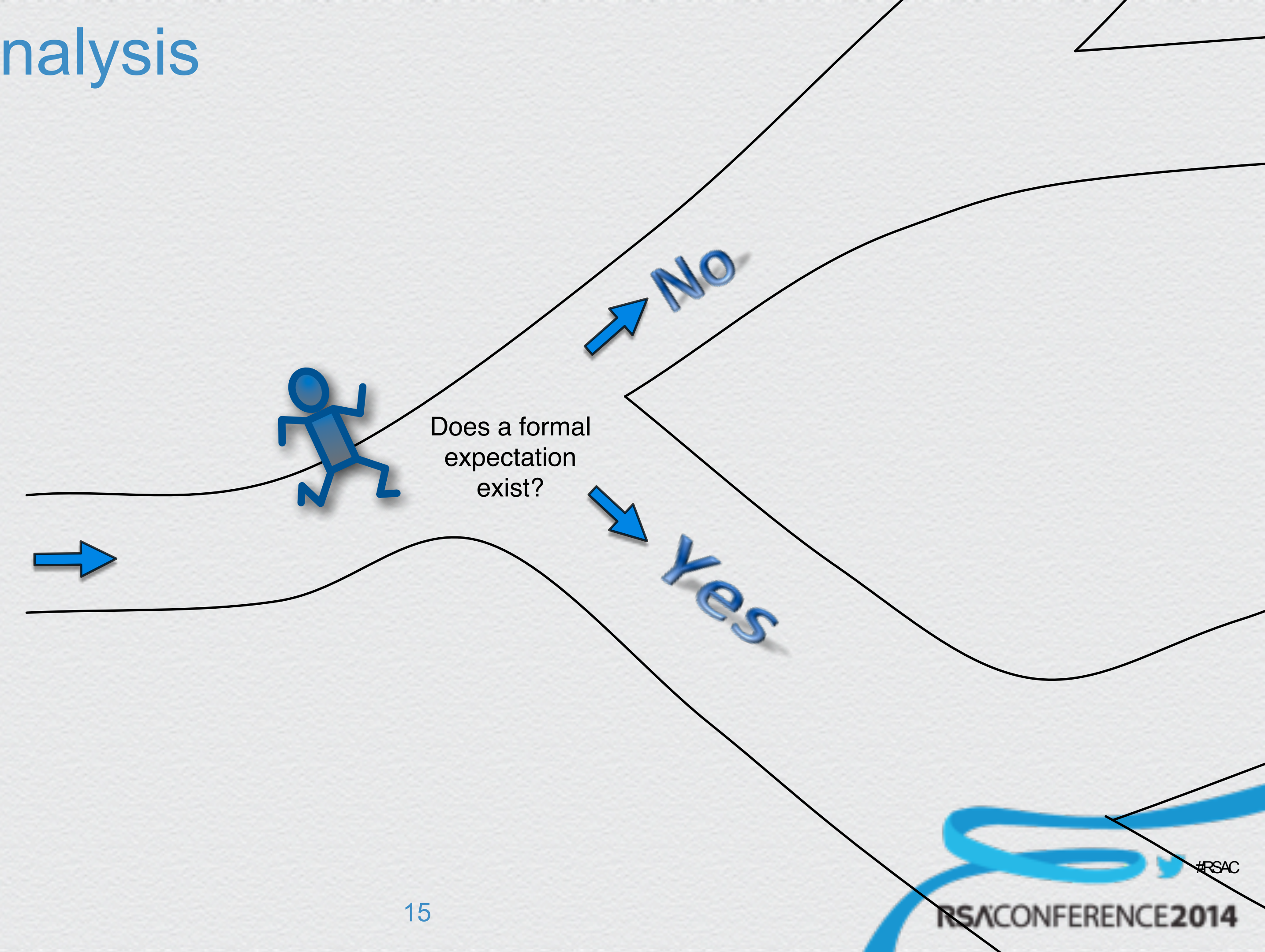
Document

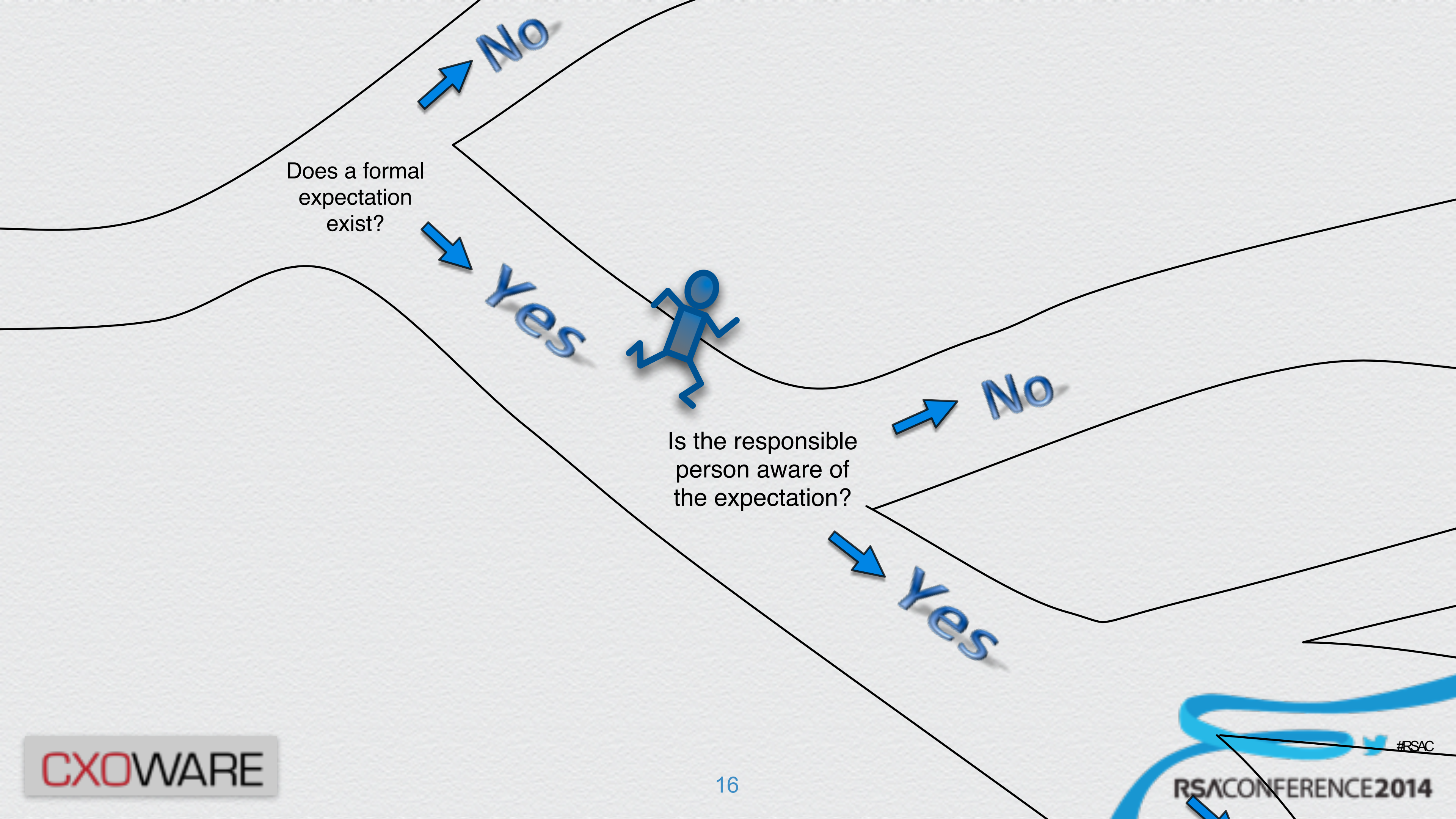
Z

Document cause

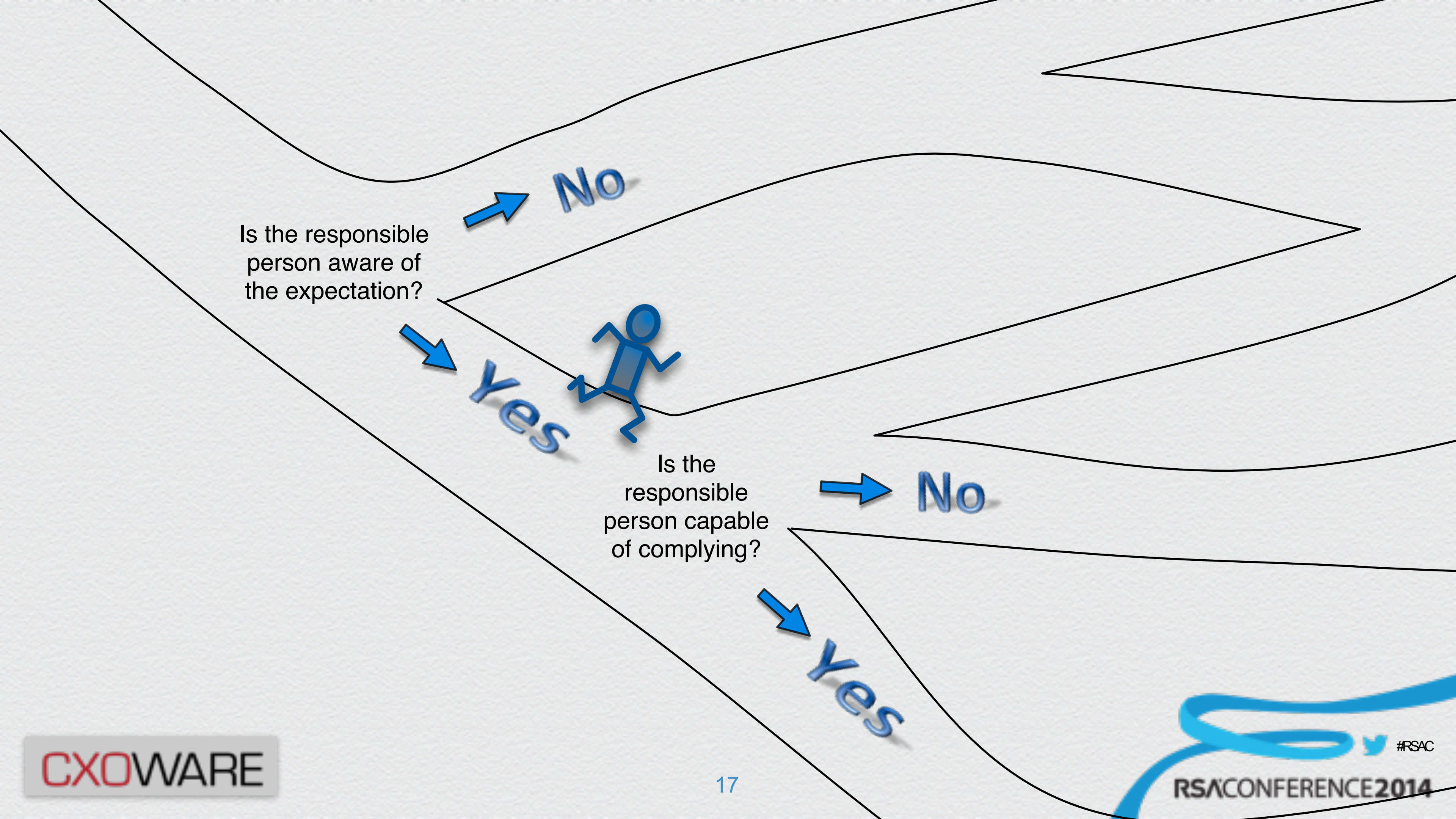
End

Root Cause Analysis Gameboard




Does a formal expectation exist?

Is the responsible person aware of the expectation?



Is the responsible person aware of the expectation?

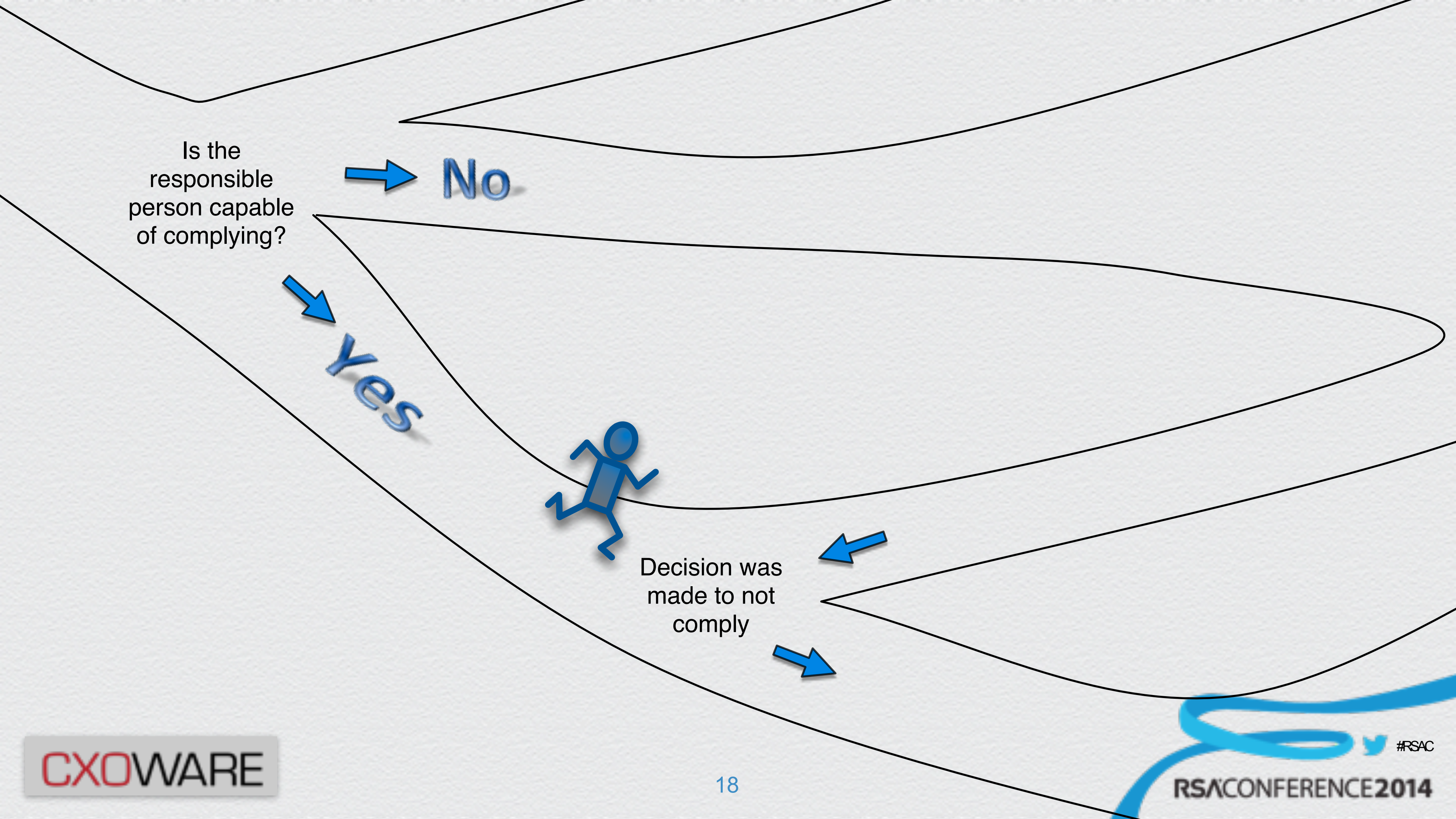
No

Yes

Is the responsible person capable of complying?

No

Yes

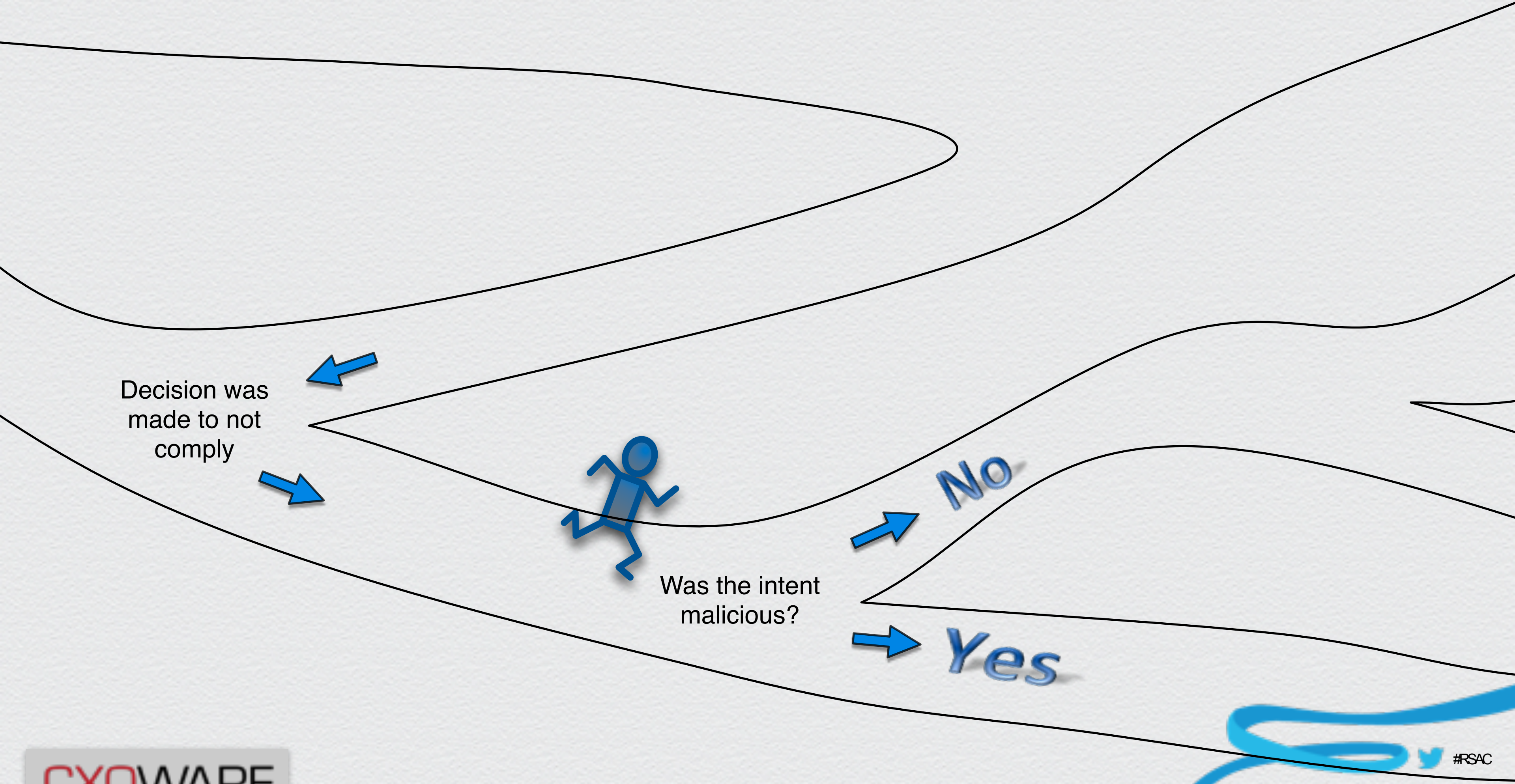


Is the responsible person capable of complying?

No

Yes

Decision was made to not comply

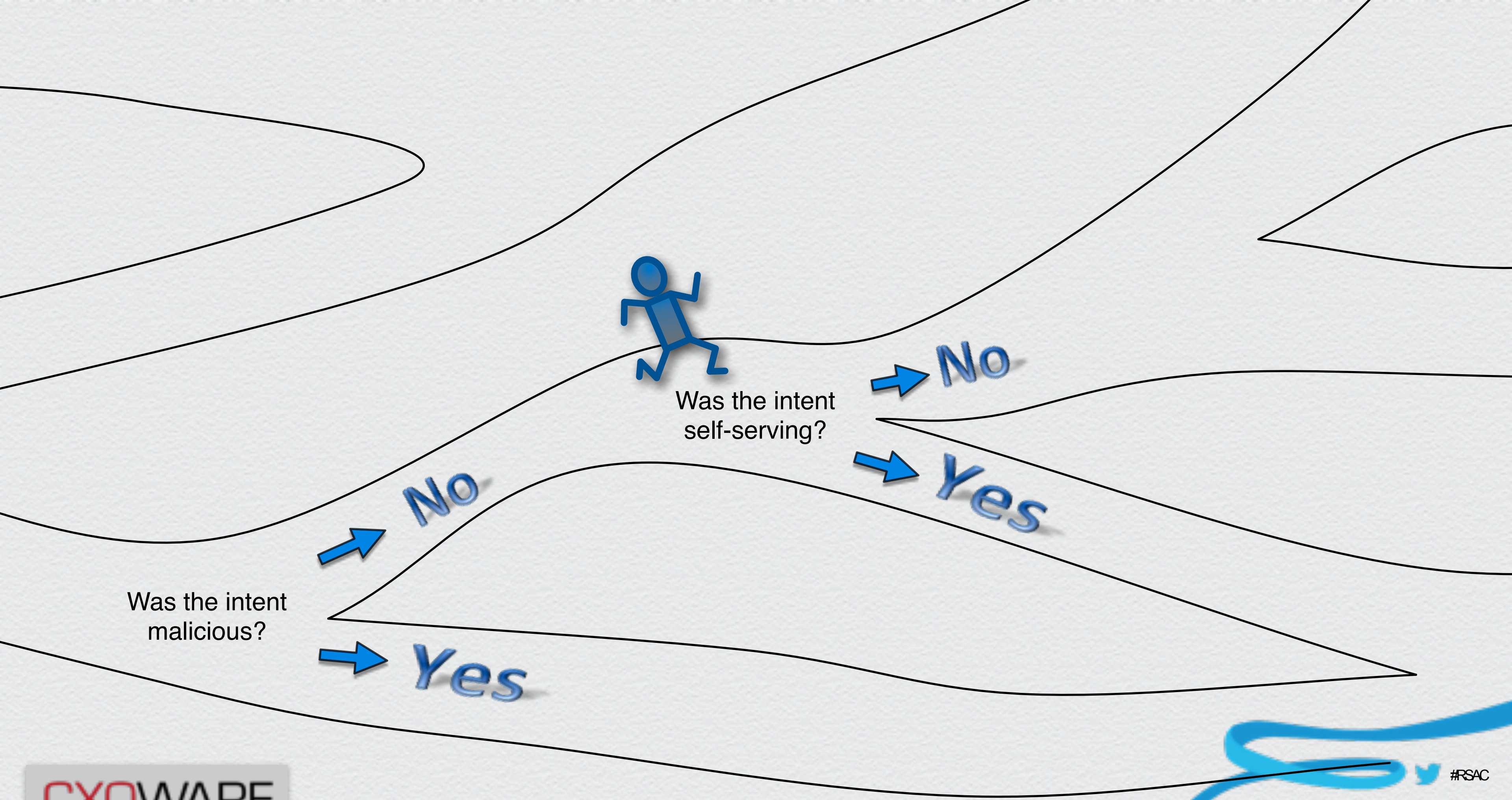


Decision was made to not comply

Was the intent malicious?

No

Yes



Was the intent malicious?

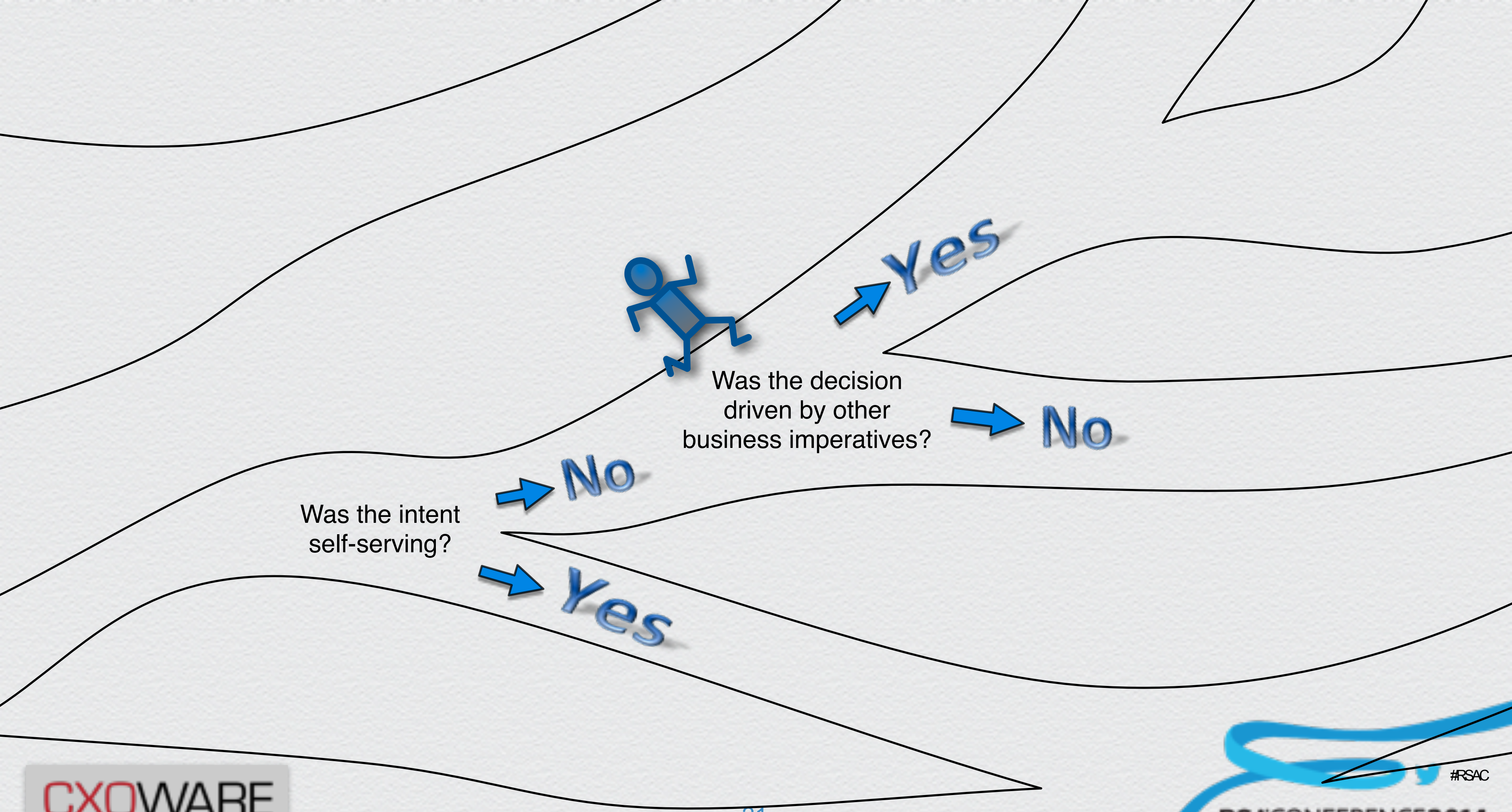
No

Yes

Was the intent self-serving?

No

Yes



Was the intent self-serving?

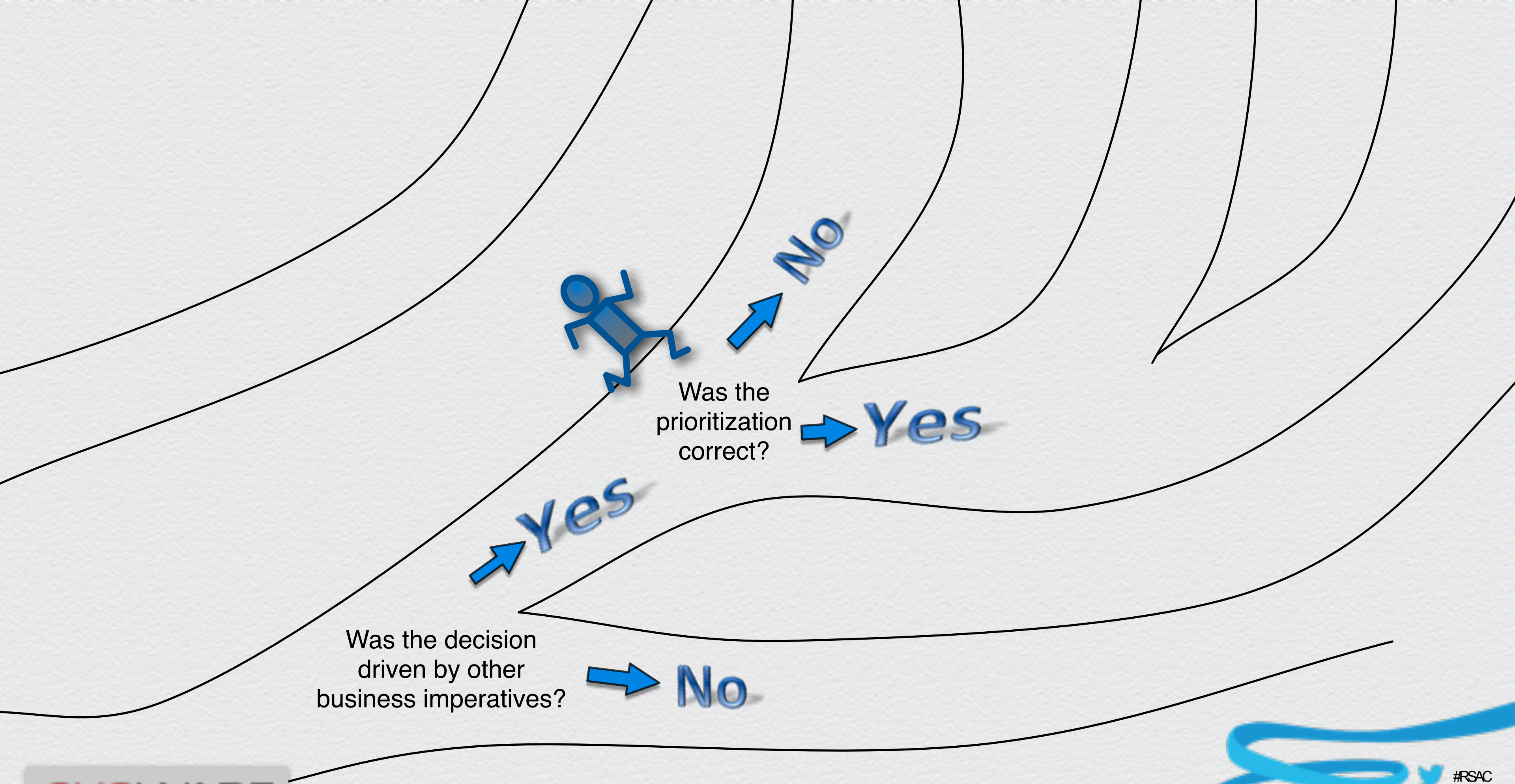
No

Yes

Was the decision driven by other business imperatives?

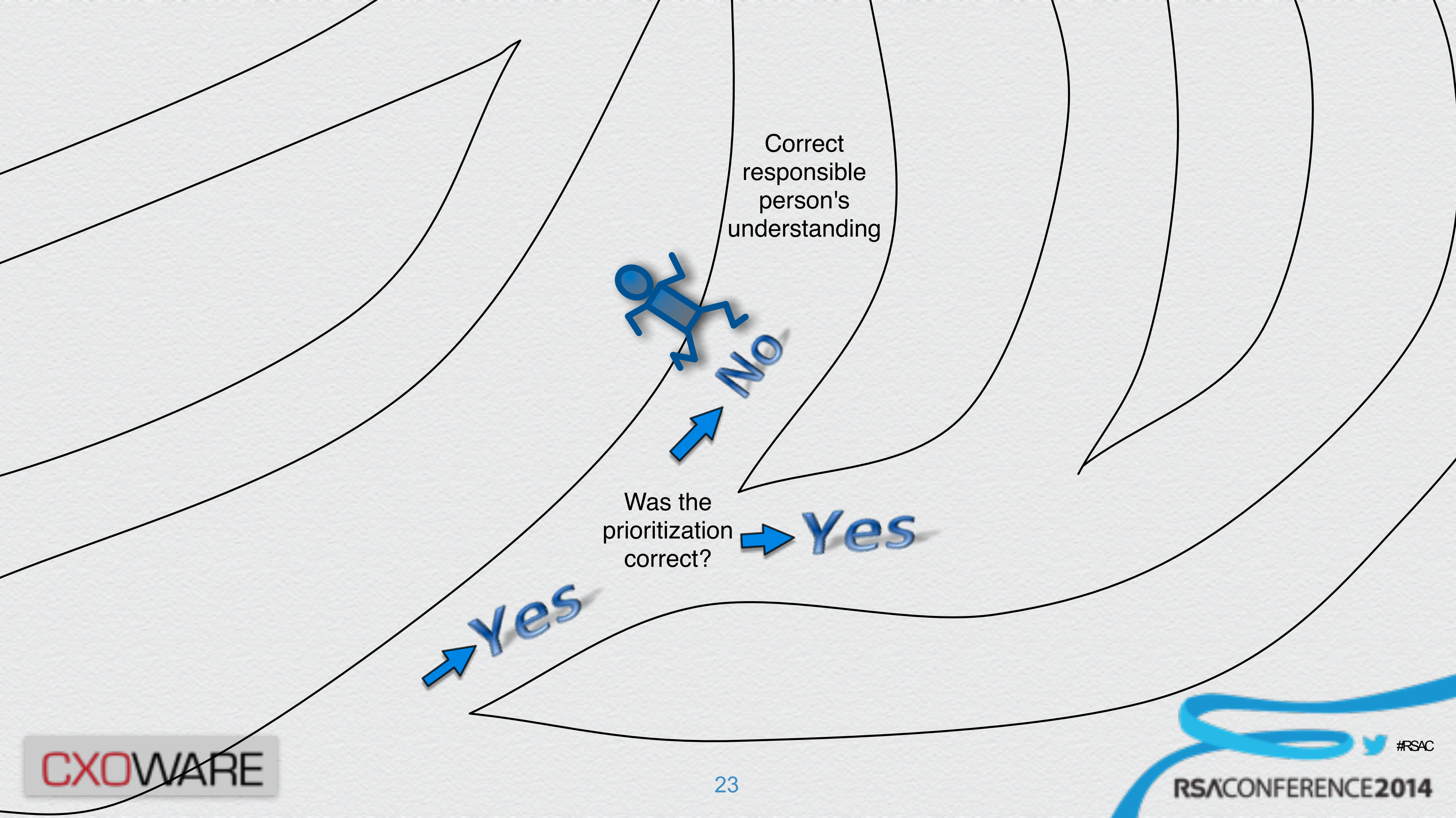
Yes

No



Was the prioritization correct?

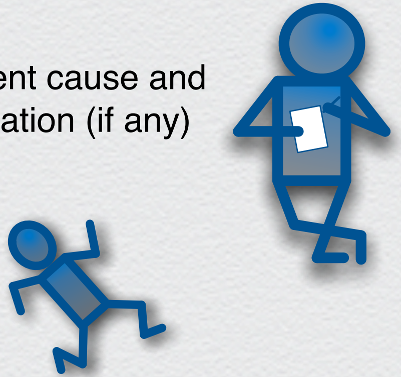
Was the decision driven by other business imperatives?



Correct responsible person's understanding

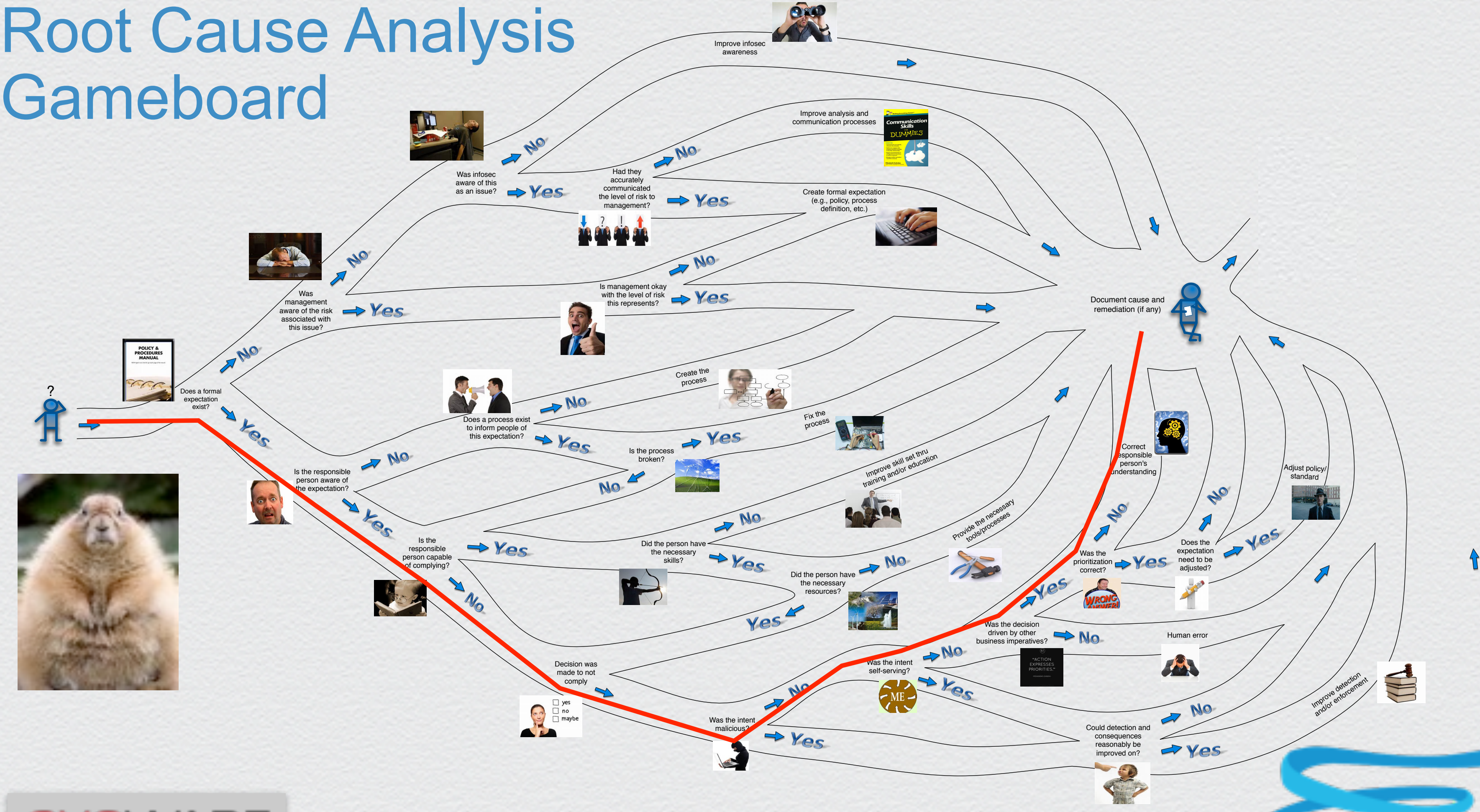
Was the prioritization correct?

Document cause and remediation (if any)



Correct responsible person's understanding

Root Cause Analysis Gameboard



Does a formal expectation exist?

No

Was management aware of the risk associated with this issue?

No

Was infosec aware of this as an issue?

No

Improve infosec awareness

Yes

Had they accurately communicated the level of risk to management?

No

Improve analysis and communication processes

Yes

Create formal expectation (e.g., policy, process definition, etc.)

Yes

Is management okay with the level of risk this represents?

No

Yes

Document cause and remediation (if any)

Yes

Is the responsible person aware of the expectation?

No

Does a process exist to inform people of this expectation?

No

Create the process

Yes

Is the process broken?

Yes

Fix the process

No

Yes

Is the responsible person capable of complying?

Yes

Did the person have the necessary skills?

No

Improve skill set thru training and/or education

Yes

Did the person have the necessary resources?

No

Provide the necessary tools/processes

Yes

No

Decision was made to not comply

☐ yes
☐ no
☐ maybe

Was the intent malicious?

No

Was the intent self-serving?

No

Was the decision driven by other business imperatives?

Yes

Was the prioritization correct?

No

Correct responsible person's understanding

Yes

Does the expectation need to be adjusted?

No

Yes

Adjust policy/ standard

No

Human error

Yes

Yes

Could detection and consequences reasonably be improved on?

No

Yes

Improve detection and/or enforcement

CXOWARE

#RSAC

RSACONFERENCE2014

Putting it to use

Putting it to use

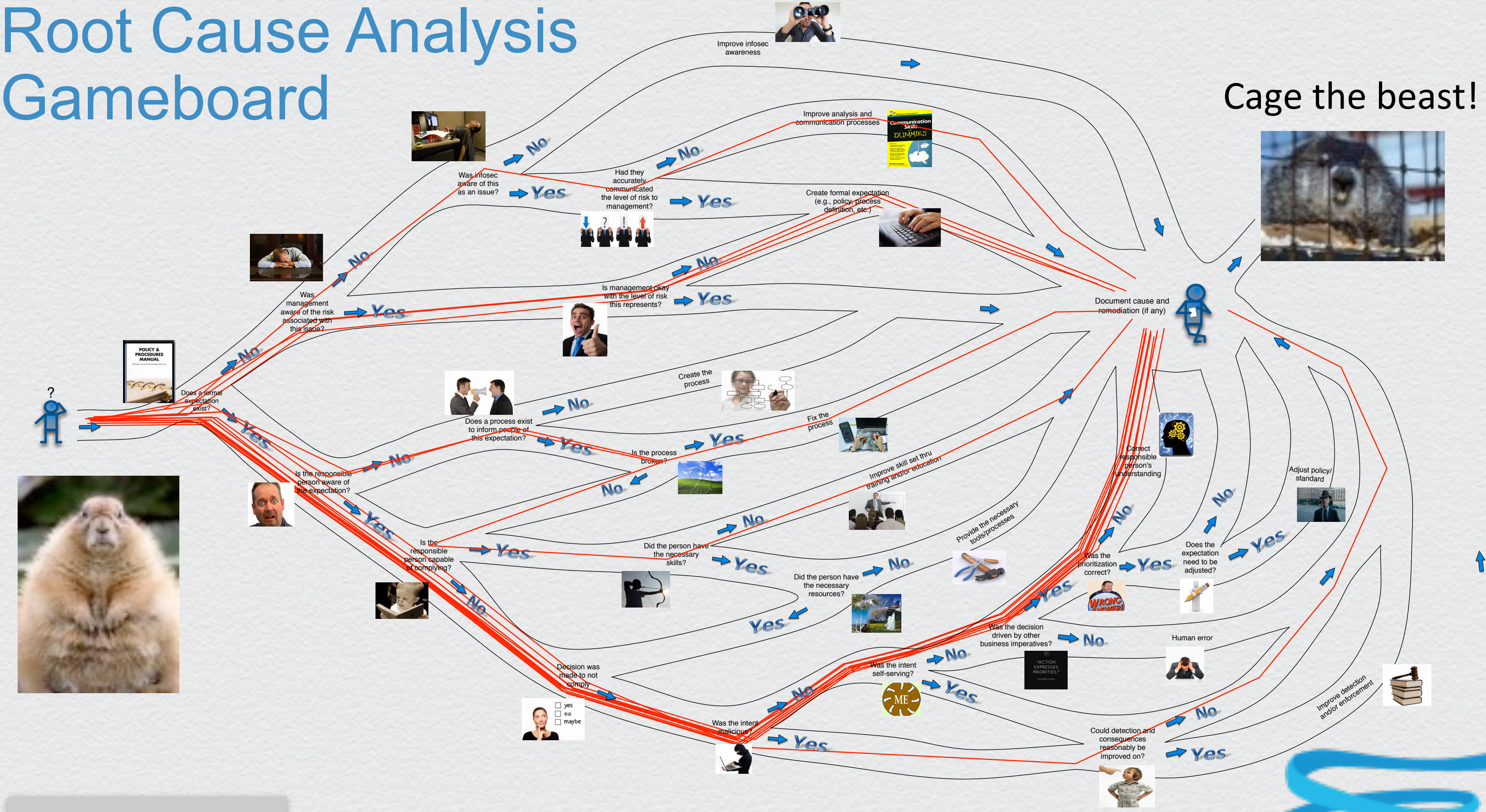
Getting to the root cause of a persistent issue is great, but it doesn't get the organization out of GHD on a larger scale...

Putting it to use

What happens if you use this root cause analysis on a portfolio of issues?

Root Cause Analysis Gameboard

Cage the beast!



?

Does a formal expectation exist?

No

Was management aware of the risk associated with this issue?

No

Was infosec aware of this as an issue?

No

Improve infosec awareness

Yes

Had they accurately communicated the level of risk to management?

No

Improve analysis and communication processes

Yes

Create formal expectation (e.g., policy, process definition, etc.)

Yes

Is management okay with the level of risk this represents?

No

Yes

Yes

Is the responsible person aware of the expectation?

No

Does a process exist to inform people of this expectation?

No

Create the process

Yes

Is the process broken?

Yes

Fix the process

No

Yes

Is the responsible person capable of complying?

Yes

Did the person have the necessary skills?

No

Improve skill set thru training and/or education

Yes

Did the person have the necessary resources?

No

Provide the necessary tools/processes

Yes

No

Decision was made to not comply

Was the intent malicious?

No

Was the intent self-serving?

No

Was the decision driven by other business imperatives?

Yes

Was the prioritization correct?

No

Correct responsible person's understanding

Yes

Does the expectation need to be adjusted?

No

Yes

Adjust policy/ standard

No

Human error

Yes

Yes

Could detection and consequences reasonably be improved on?

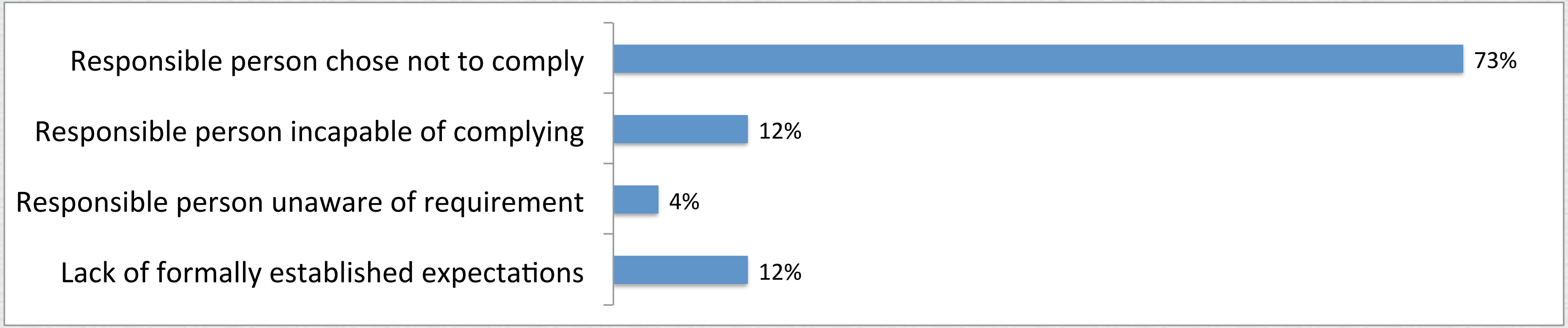
No

Yes

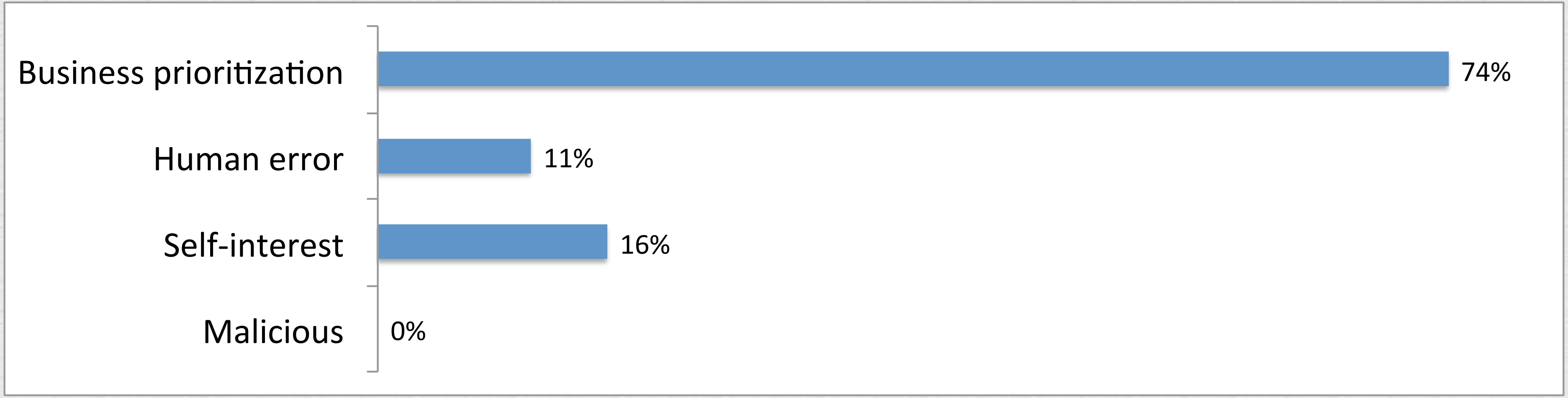
Improve detection and/or enforcement

Document cause and remediation (if any)

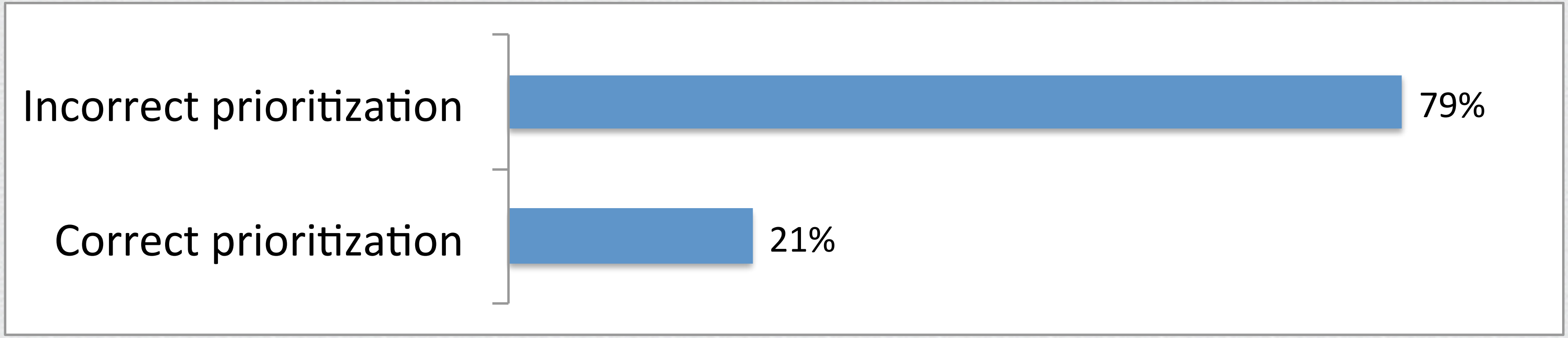
You might get something like this...



Digging in...


Business prioritization
74%
Human error
11%
Self-interest
16%
Malicious
0%

Digging in some more...



Points of integration

- Audit and security test results
- Project management
- CIRT process

Segmenting analyses and results

- Primary root causes may vary by...
  - Department / line of business
  - Technology

Summary

Summary

- GHD results from not recognizing and dealing with root causes
- As a rule, we remediate symptoms rather than root causes
- Knowing the questions to ask makes all the difference
- Root causes are often systemic
  - Portfolio analysis allows us to recognize and treat systemic problems
- Integration into existing processes allows you to acquire, track, and leverage data over time, which allows you to...
- Cage the beast!

Questions?