32nd ISMOR

Analysing the Impact of a Cyber Attack using Economic Value Chains

Presenter: Dr. Andrew Barwell
Consultant
Solutions & Business Modelling
QinetiQ Ltd

Email: ADBarwell@QinetiQ.com

Date: 23rd July 2015

Contents

- Overview of EVC Technique
- EVC Study Analysis
- Conclusions

Potted History of EVC

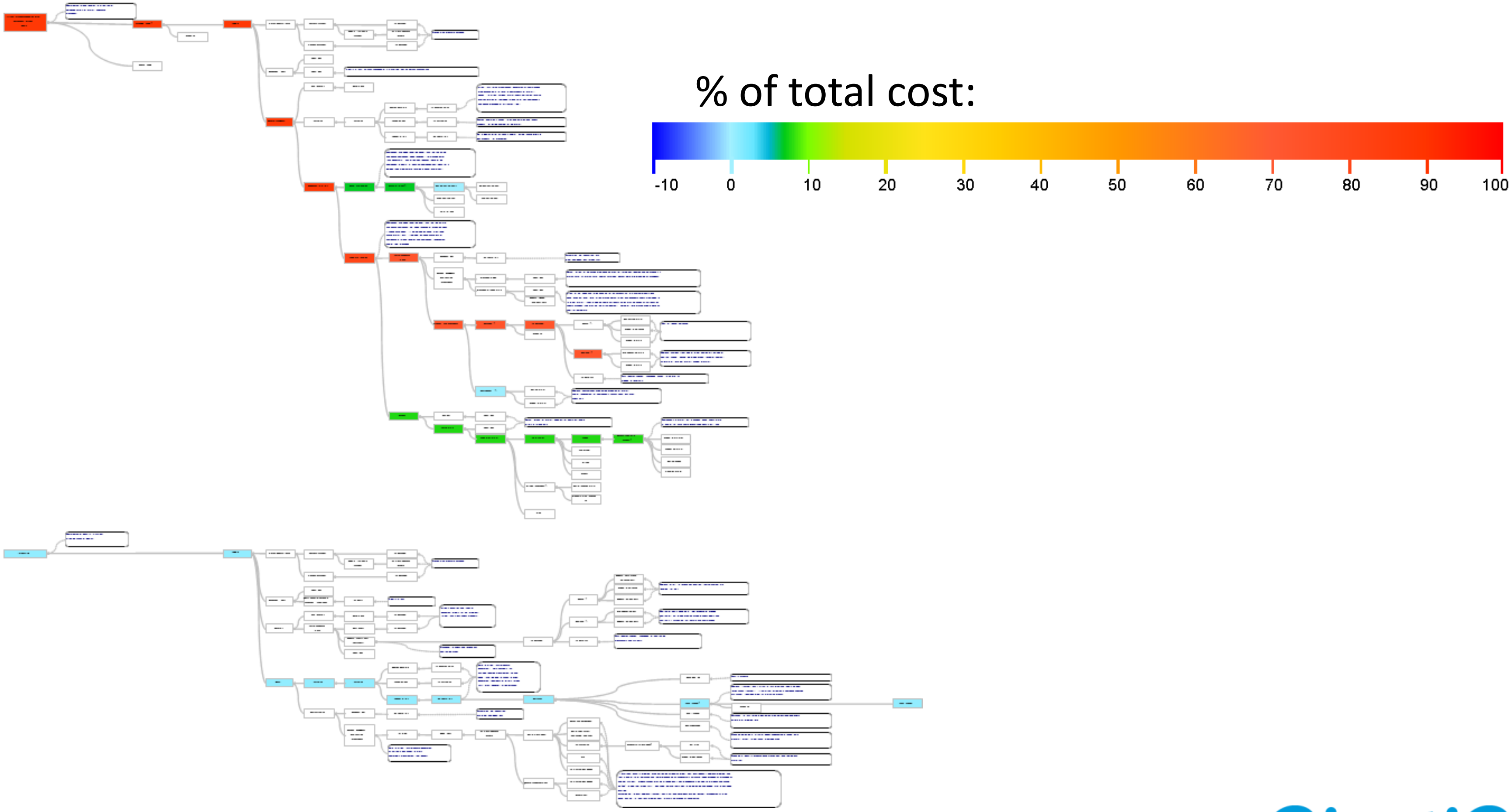
- EVC, or *Economic Value Chains* is a cost modelling method developed by Colin Sandall of QinetiQ
- EVC began life in 2012 as Centre For Defence Enterprise study to cost impact of cyber attacks
- Subsequent 2013 study successfully tested EVC as an analytic costing tool
- The technique developed further during the current (2014) study to reflect more complex scenarios
- It currently exists as an Excel-based tool, but QinetiQ are in the process of producing a bespoke solution.

EVC Overview

- EVC model and output is centered on the Diagram – an enhanced causal map.

EVC Overview

- EVC Diagram represents **decomposition of cost** from output node (on the left) to individual input nodes (on the right)



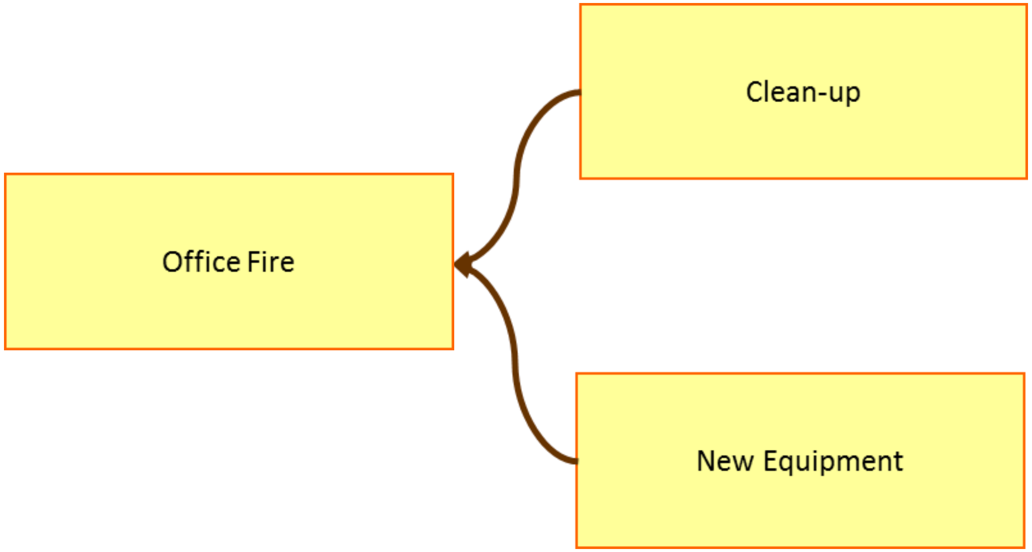
EVC Technique – Building the Diagram

- Example: what are the cost impacts of an office fire?

Office Fire

EVC Technique – Building the Diagram

- First we work out the likely cost areas



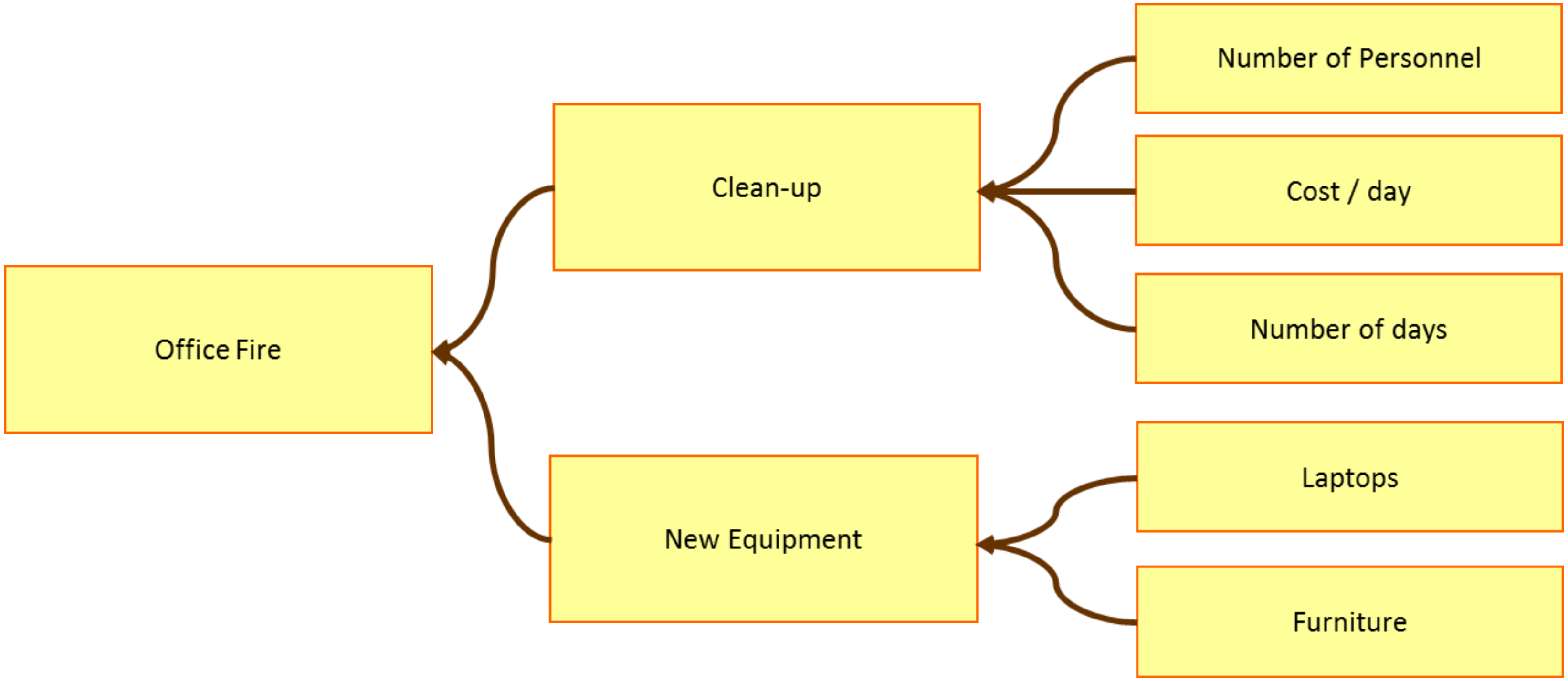
Clean-up

Office Fire

New Equipment

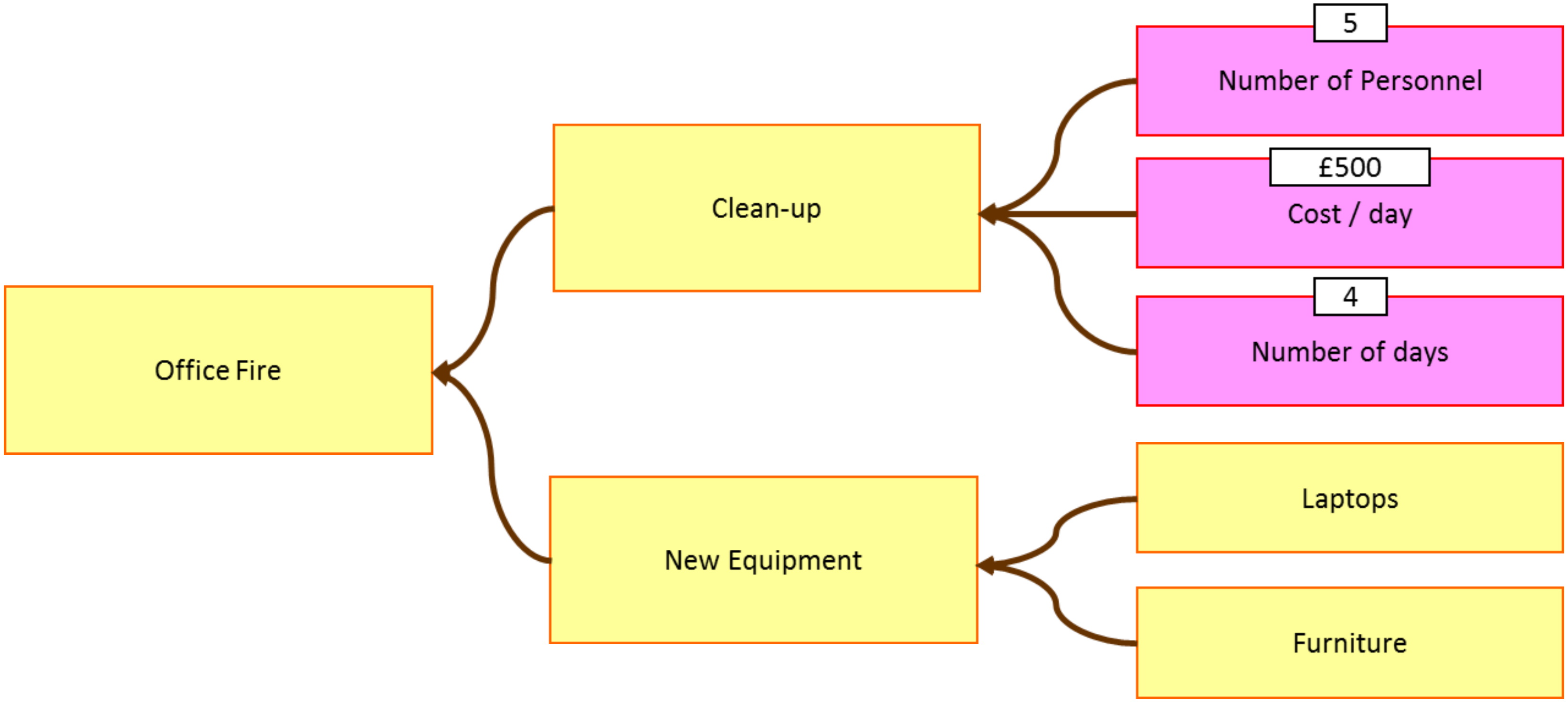
EVC Technique – Building the Diagram

- New nodes are added as our understanding develops



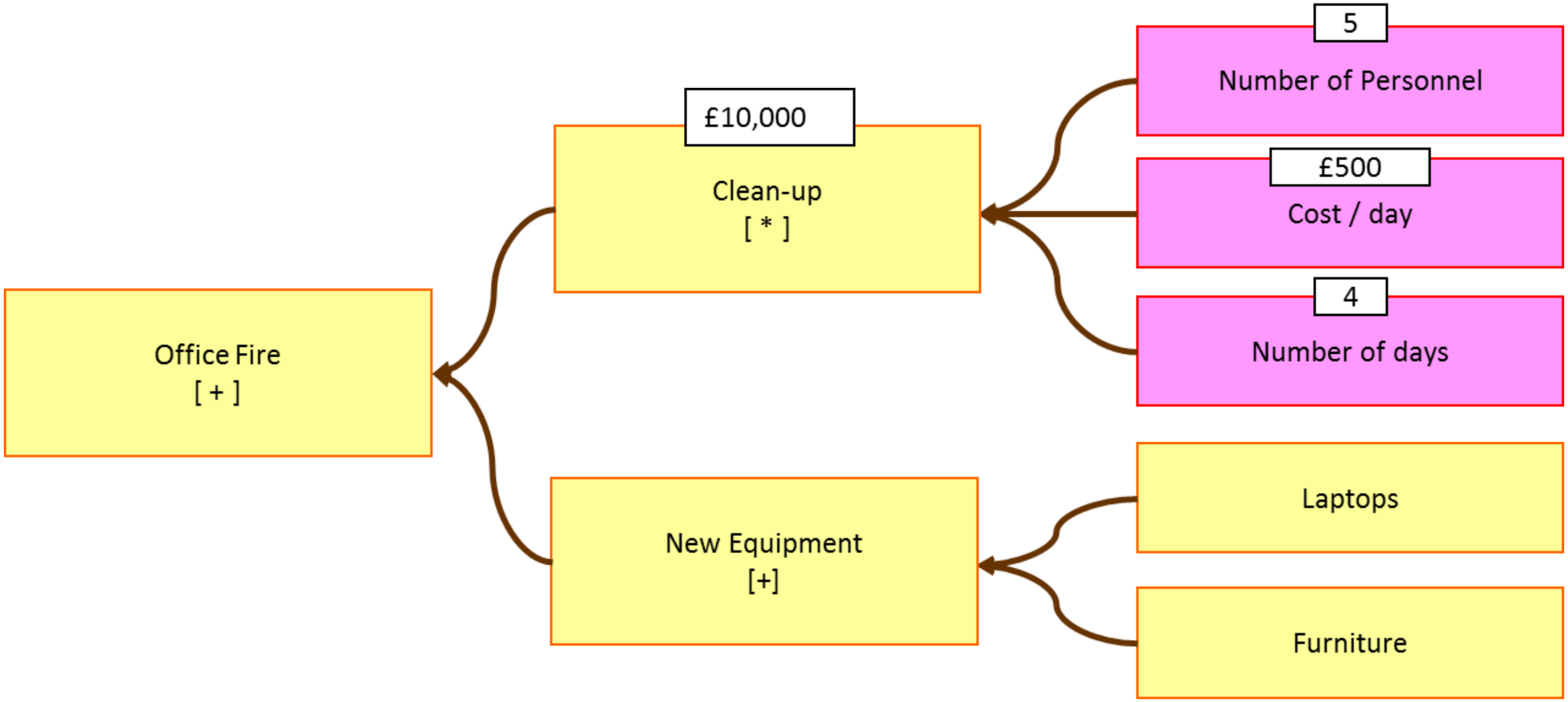
EVC Technique – Building the Diagram

- Pink nodes show where inputs are required
- Baseline costs not needed – we only need to know the **cost delta**; i.e. the additional costs incurred as a result of the event



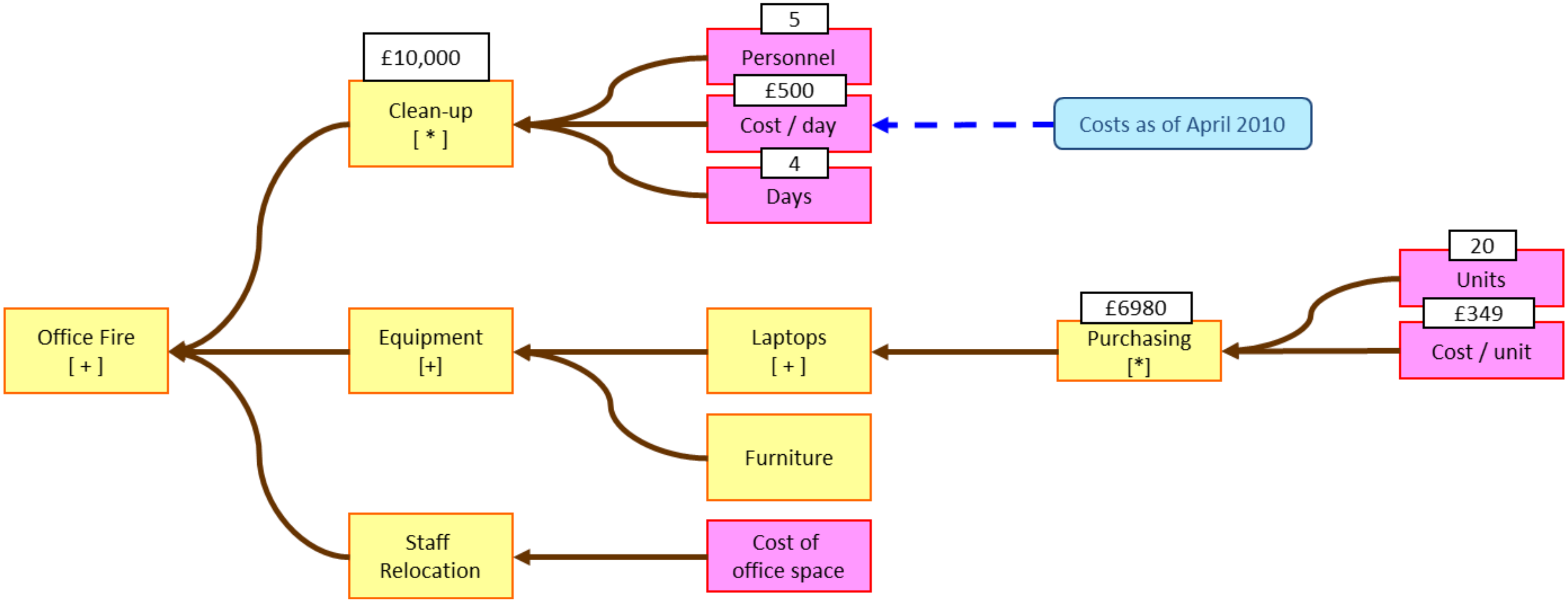
EVC Technique – Building the Diagram

- Each (non-input) node has an **operator** for combining child nodes (e.g. +, *, -, /)



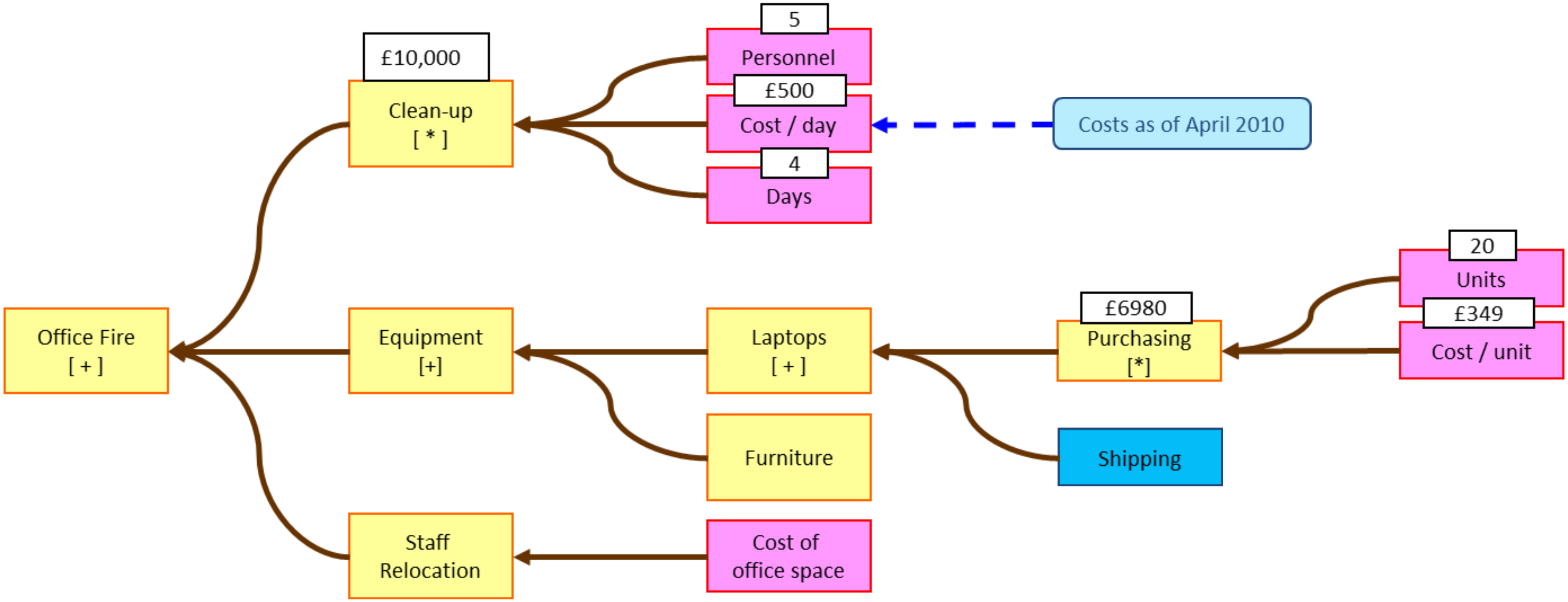
EVC Technique – Building the Diagram

- **Comment nodes** provide validation evidence and audit trail



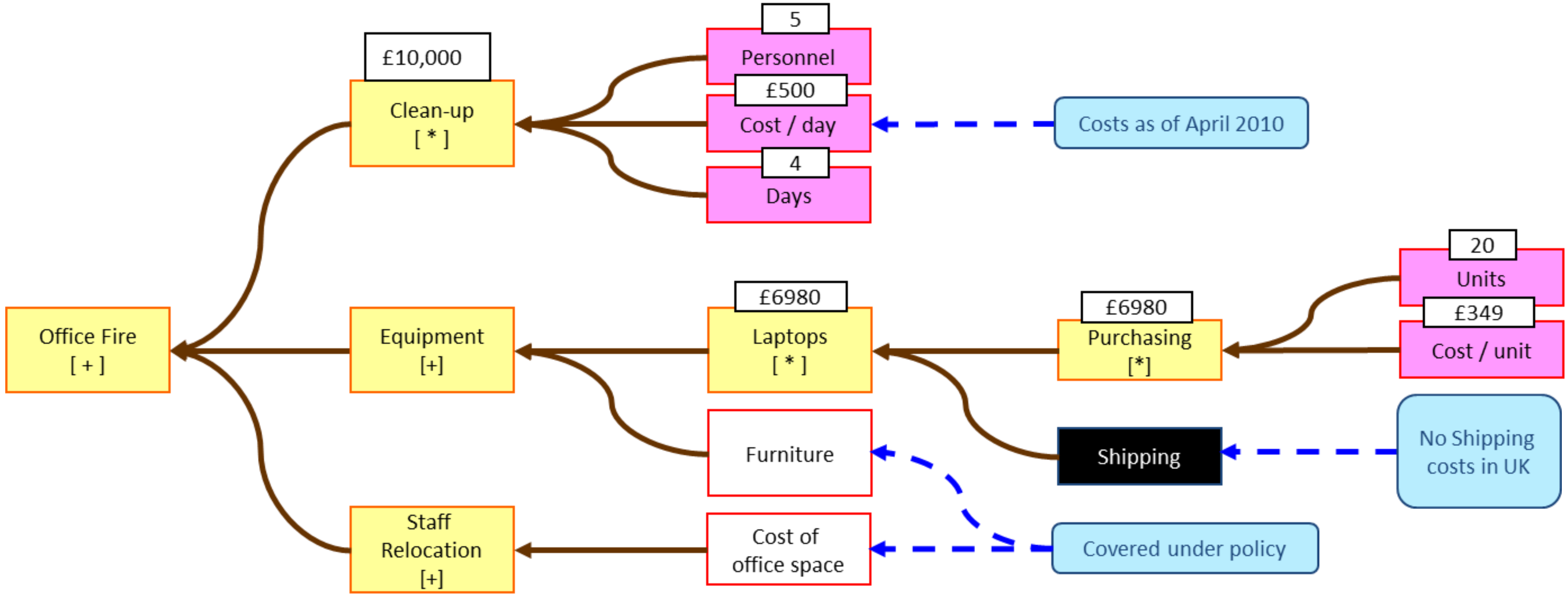
EVC Technique – Building the Diagram

- **Module nodes** allow repeated use of common elements, such as Shipping costs.



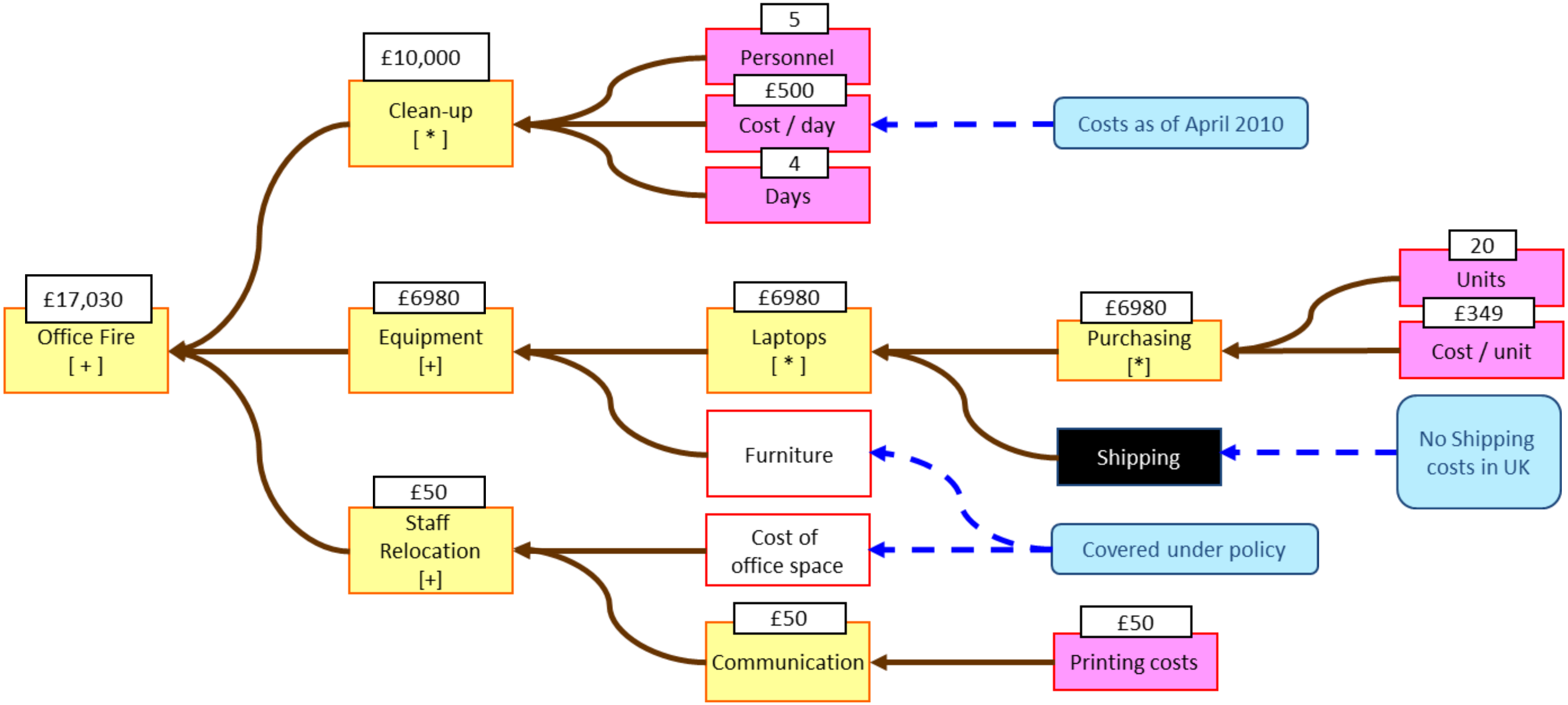
EVC Technique – Building the Diagram

- White and black nodes are two different types of zero cost node
- We include these to show that the cost element has been considered



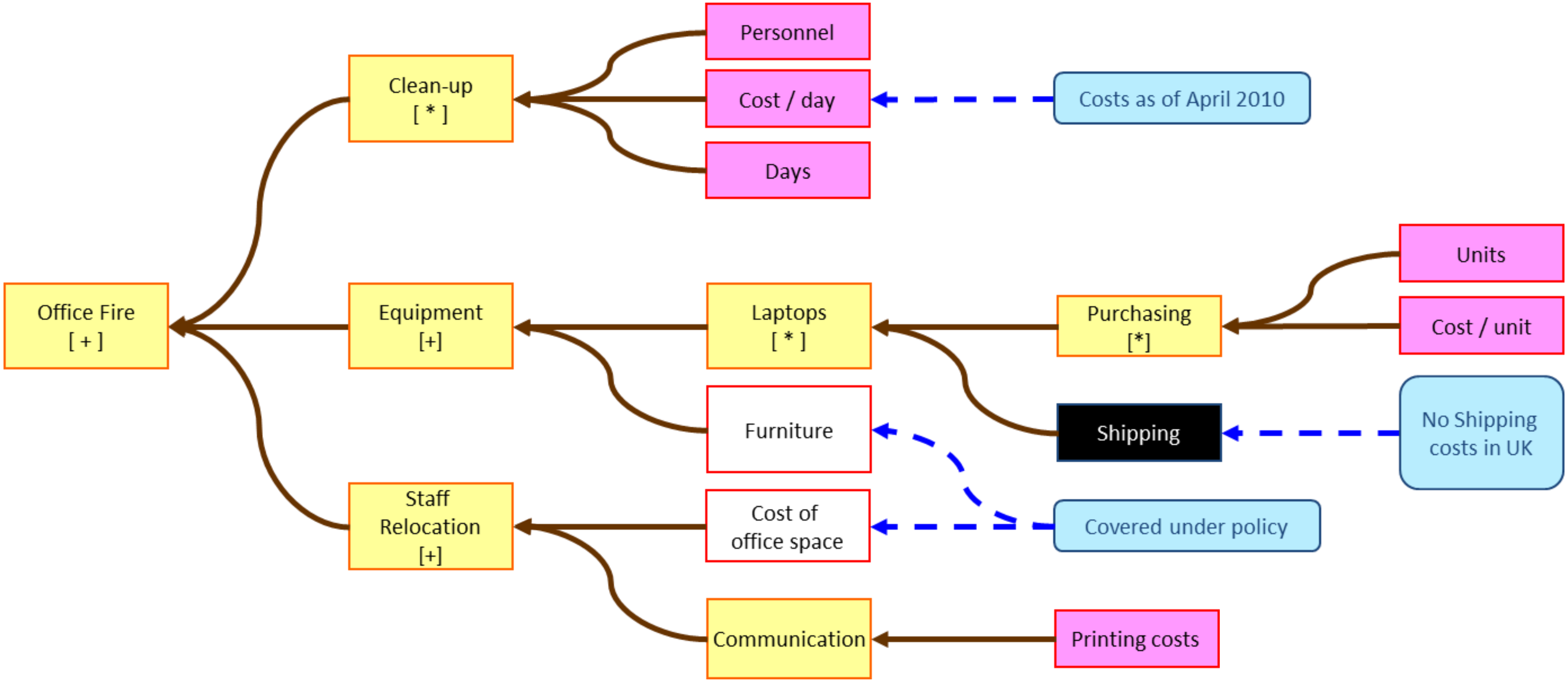
EVC Technique – Building the Diagram

- Input values **aggregate through Diagram** to give vignette cost.



EVC Technique – Running the Model

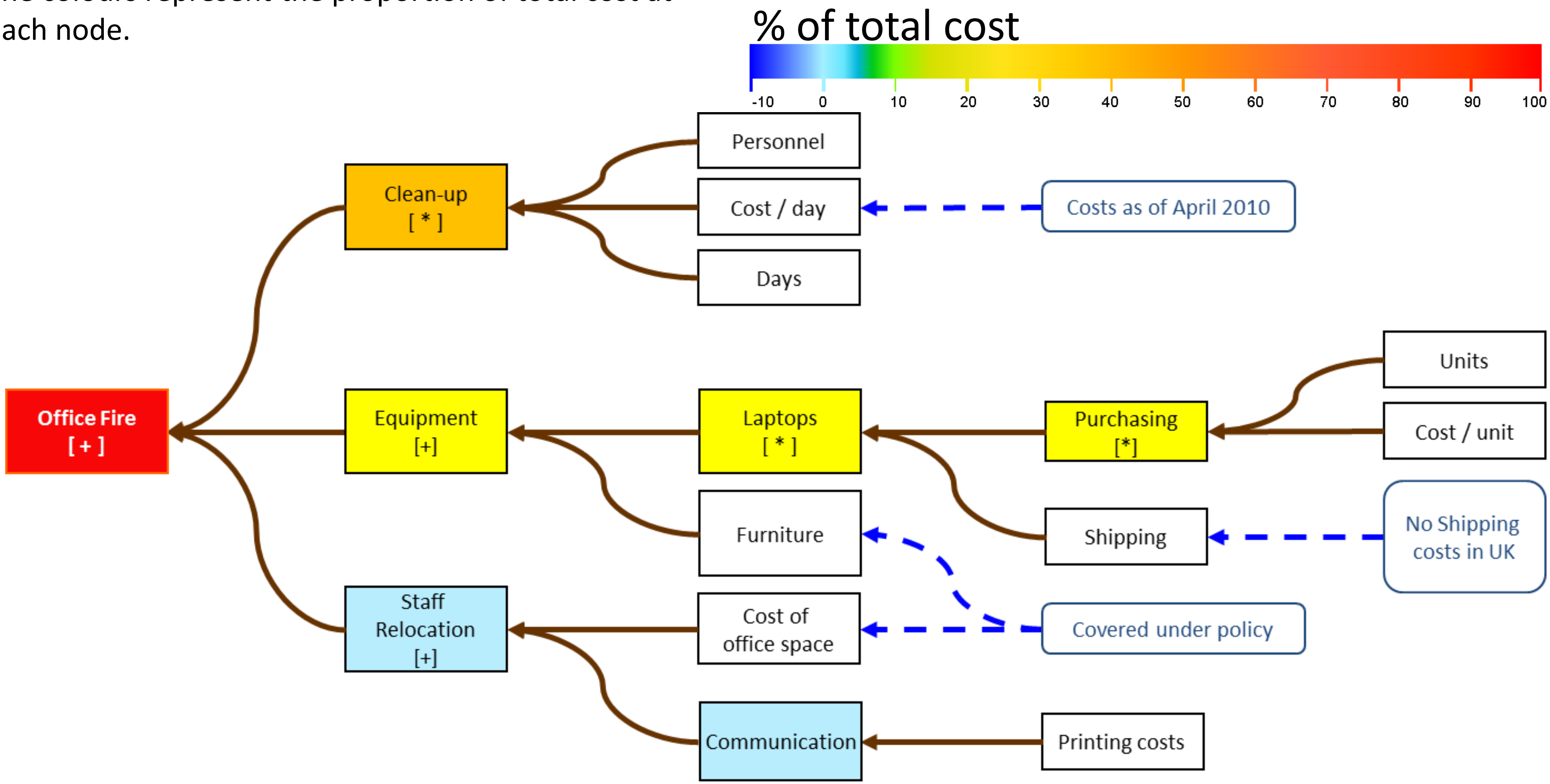
- Node colour highlights which elements drive the overall cost…



EVC Technique – Running the Model

- Node colour highlights which elements drive the overall cost…

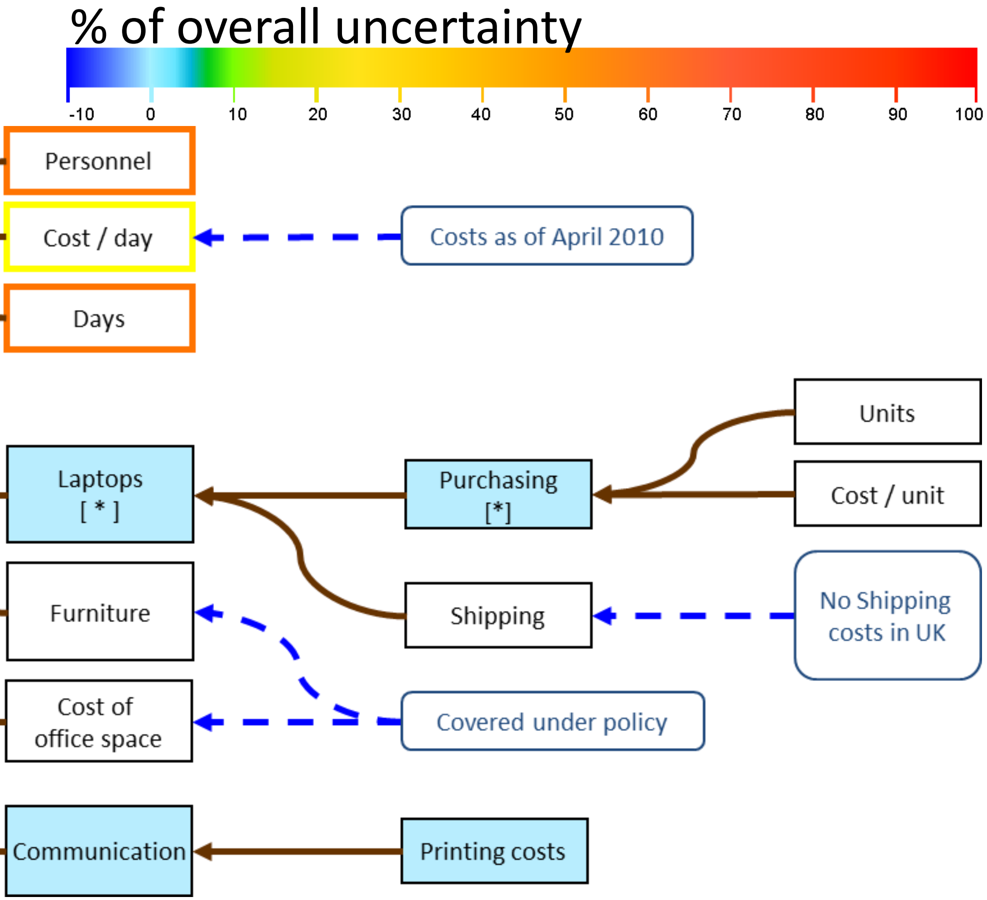
The colours represent the proportion of total cost at each node.



EVC Technique – Running the Model

- … and where greatest uncertainty lies

(3-point estimates for each input are captured and a Monte Carlo simulation is run; uncertainty at each node is the difference between the minimum and maximum cost over the entire simulation)



Contents

- Overview of EVC Technique
- EVC Study Analysis
- Summary

Overview of the Study

The following application of EVC is from a study conducted by QinetiQ for Dstl. Details of the platform and scenario are sensitive, but many of the effects are widely applicable.

Study Aim:

- Investigate the impact of a cyber-attack on a platform IT system
- Quantify the impact of the attack in economic terms
- Identify drivers of overall cost and areas of uncertainty

Cyber-Attack Effects

Primary effects (those produced by a cyber attack):

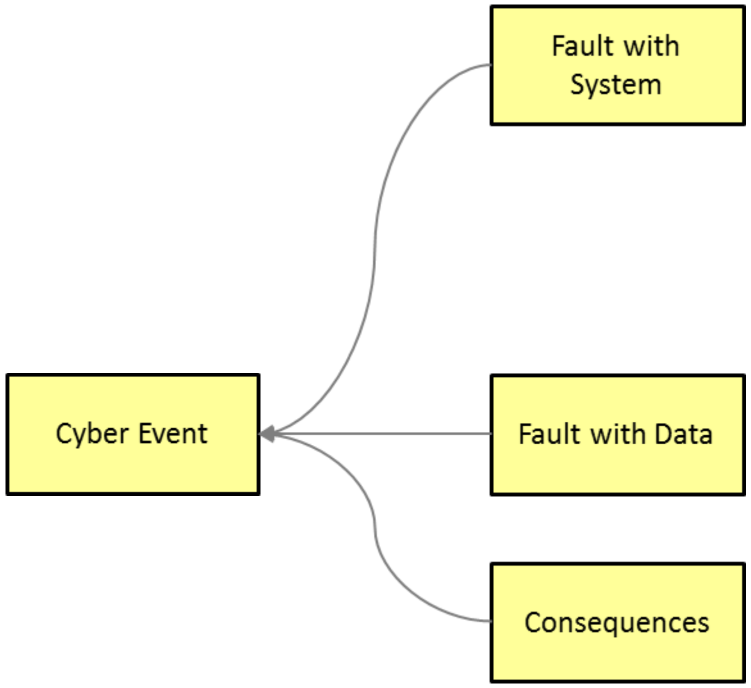
- Availability – denial of service (DoS)
- Integrity – data compromised
- Confidentiality – data acquired by enemy forces (out of scope).

Secondary effects (those produced as a result of primary effects):

- Operational impact - Availability / operational limitations
- Human factors – loss of confidence in IT system and (thus) in platform
- Political impact due to loss of platform availability.

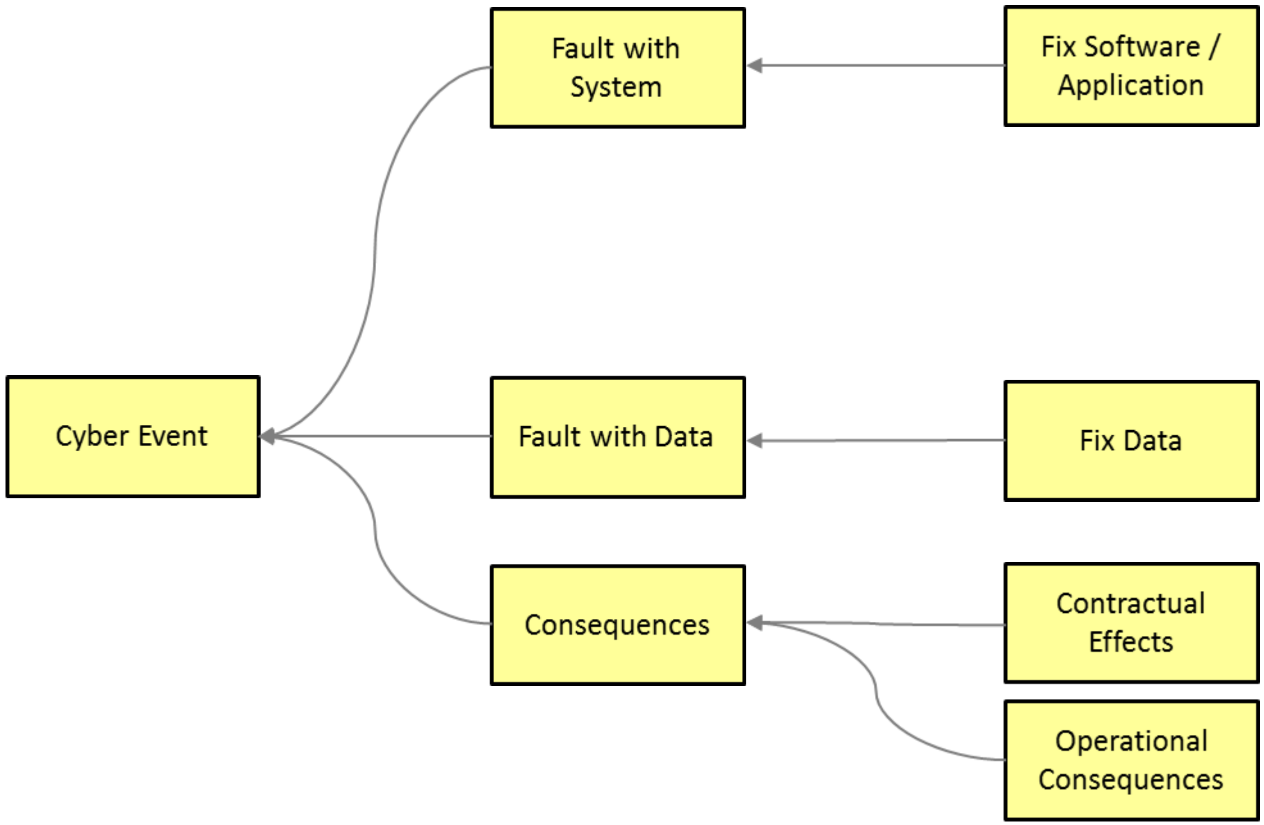
EVC Cyber-Attack Analysis

Top-level EVC:



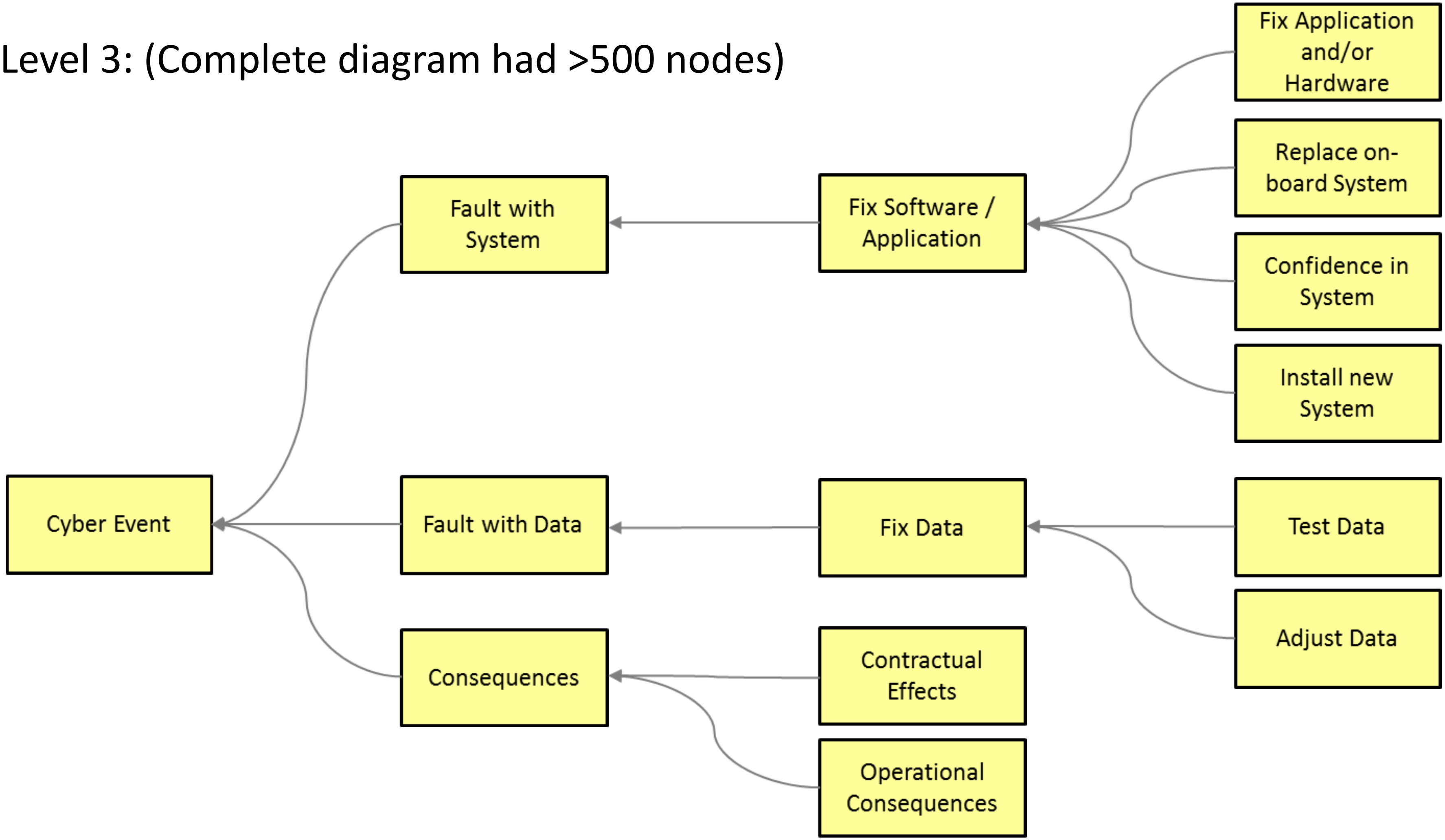
EVC Cyber-Attack Analysis

Level 2:



EVC Cyber-Attack Analysis

Level 3: (Complete diagram had >500 nodes)



Sub-Scenario “Strands”

The precise nature of the impact of an attack will depend upon a number of discriminating factors:

•**Has an attack actually occurred?** If not, costs may be incurred even if it is *believed* an attack has occurred.

•**Has the attack been detected?** Detection will increase response but may limit duration/scope of attack.

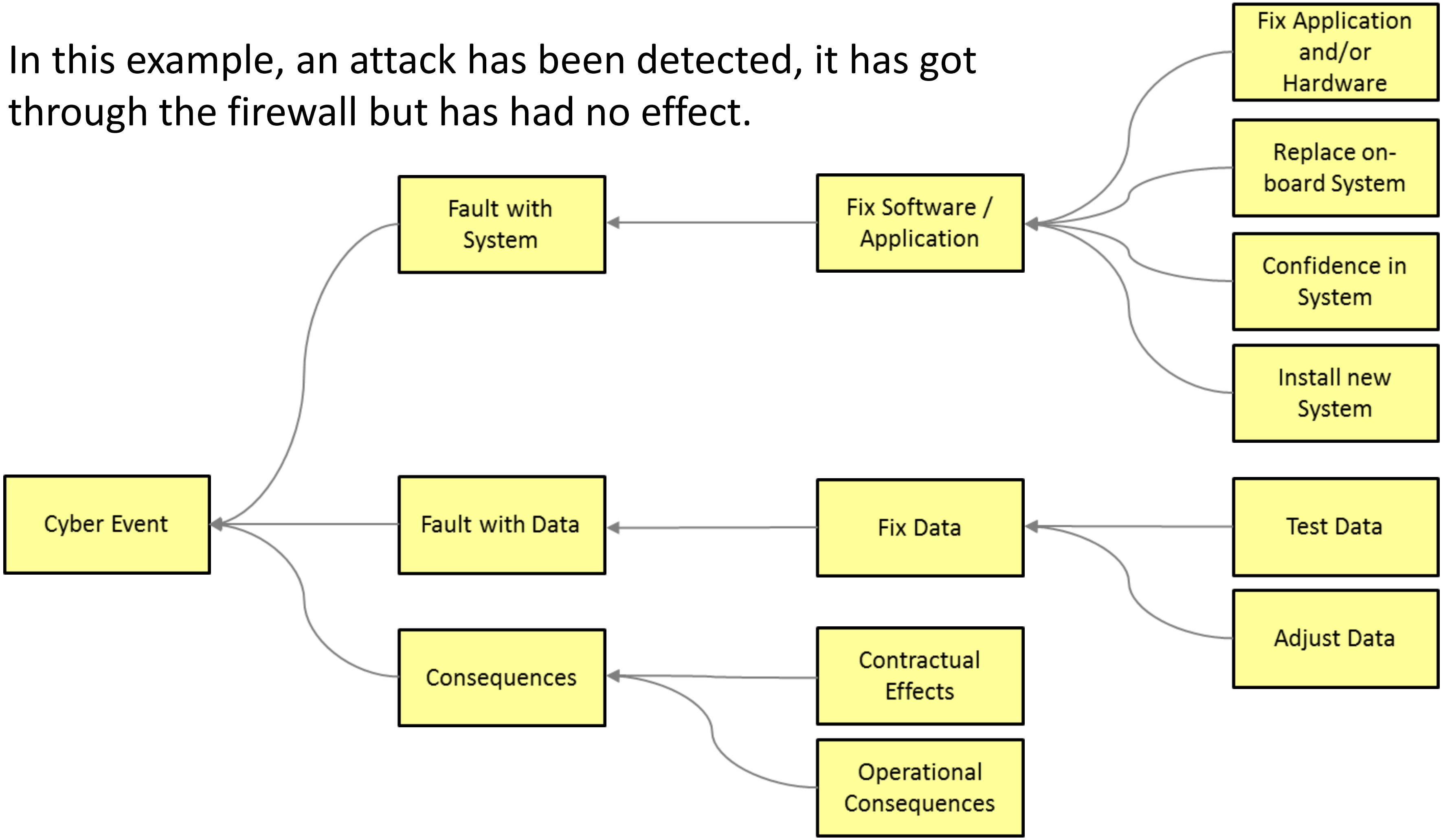
•**What type of attack has occurred?** A denial-of-service attack will have different effects from those of an integrity attack.

We will look at two sub-scenario strands, and also look at how mitigation strategies can be explored.

Absolute costs are omitted for security reasons, but total costs range from a few thousand pounds to tens of millions.

1. Attack detected not blocked but has no effect

In this example, an attack has been detected, it has got through the firewall but has had no effect.



Cyber Event

Fault with System

Fault with Data

Consequences

Fix Software / Application

Fix Data

Contractual Effects

Operational Consequences

Fix Application and/or Hardware

Replace on-board System

Confidence in System

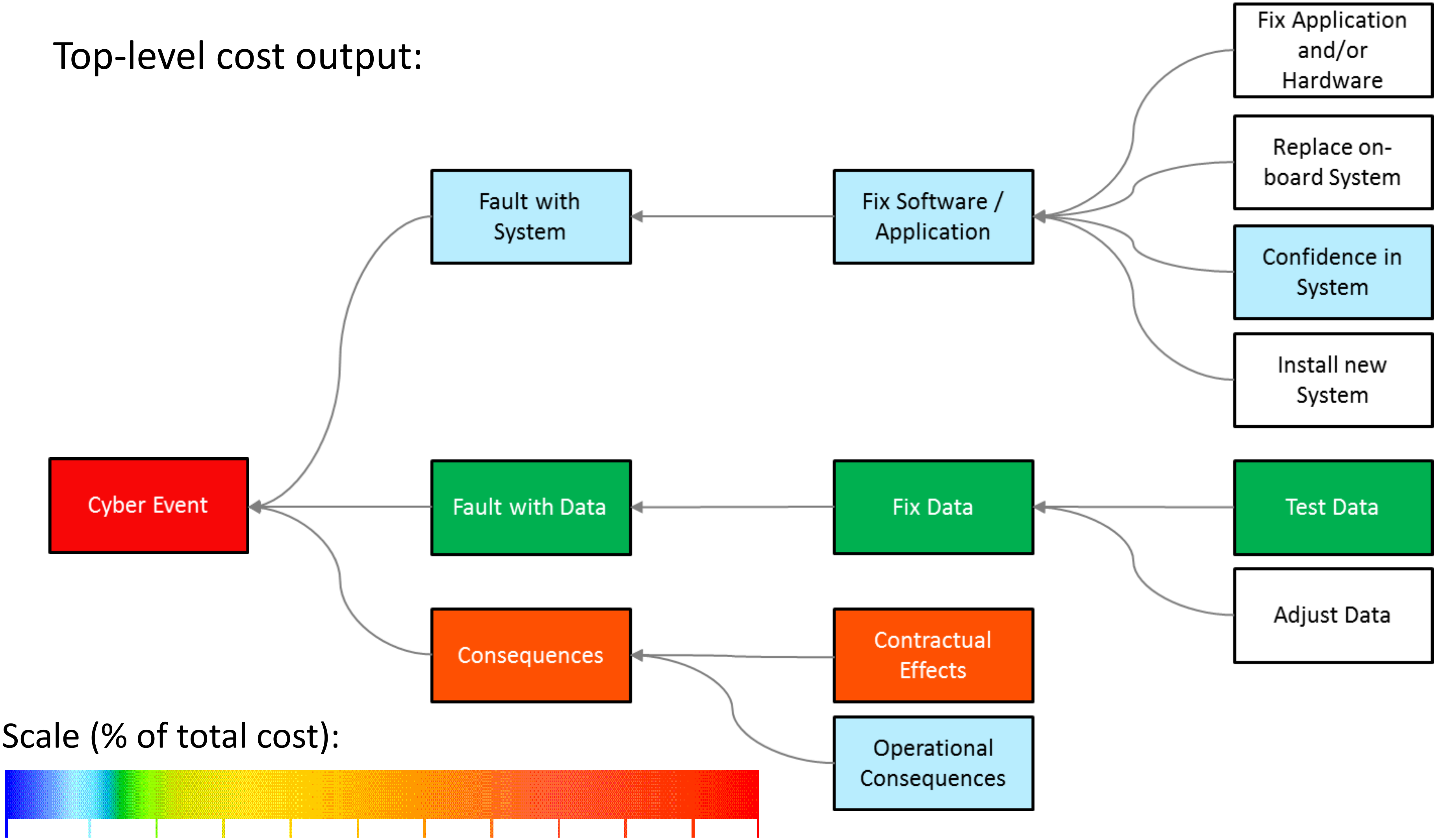
Install new System

Test Data

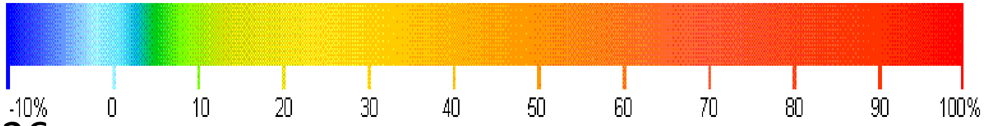
Adjust Data

1. Attack detected not blocked but has no effect

Top-level cost output:

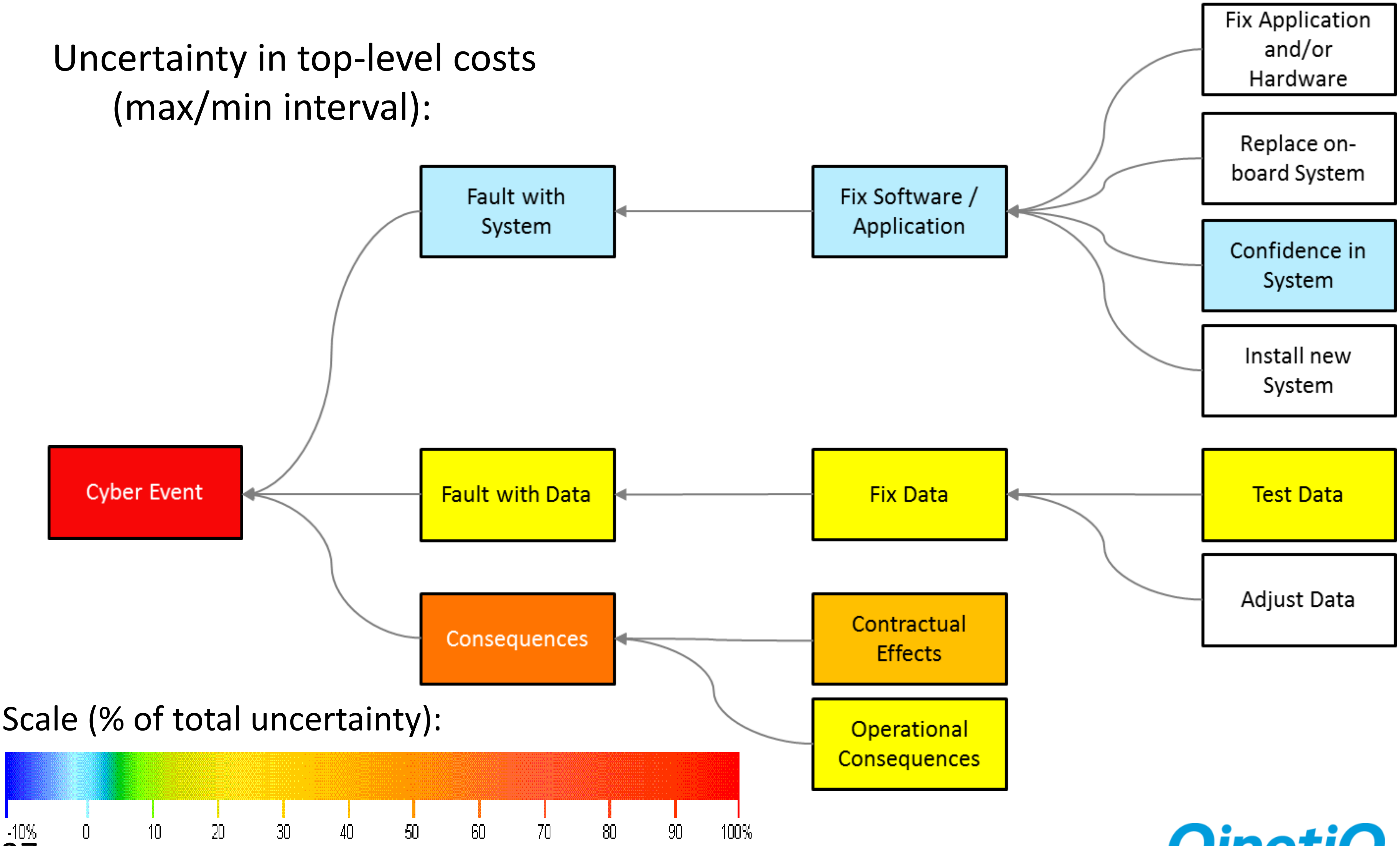


Scale (% of total cost):



1. Attack detected not blocked but has no effect

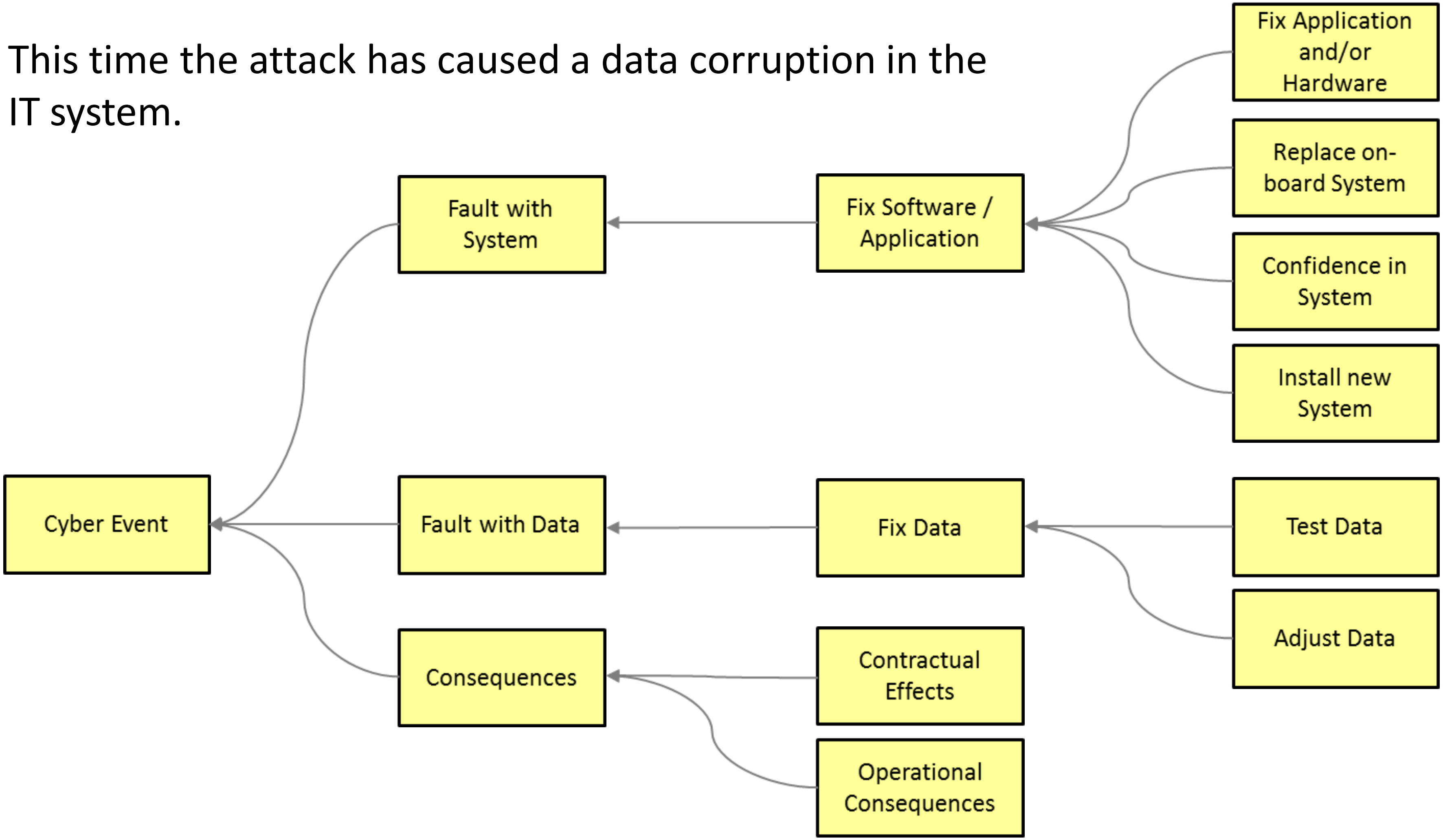
Uncertainty in top-level costs (max/min interval):



Scale (% of total uncertainty):

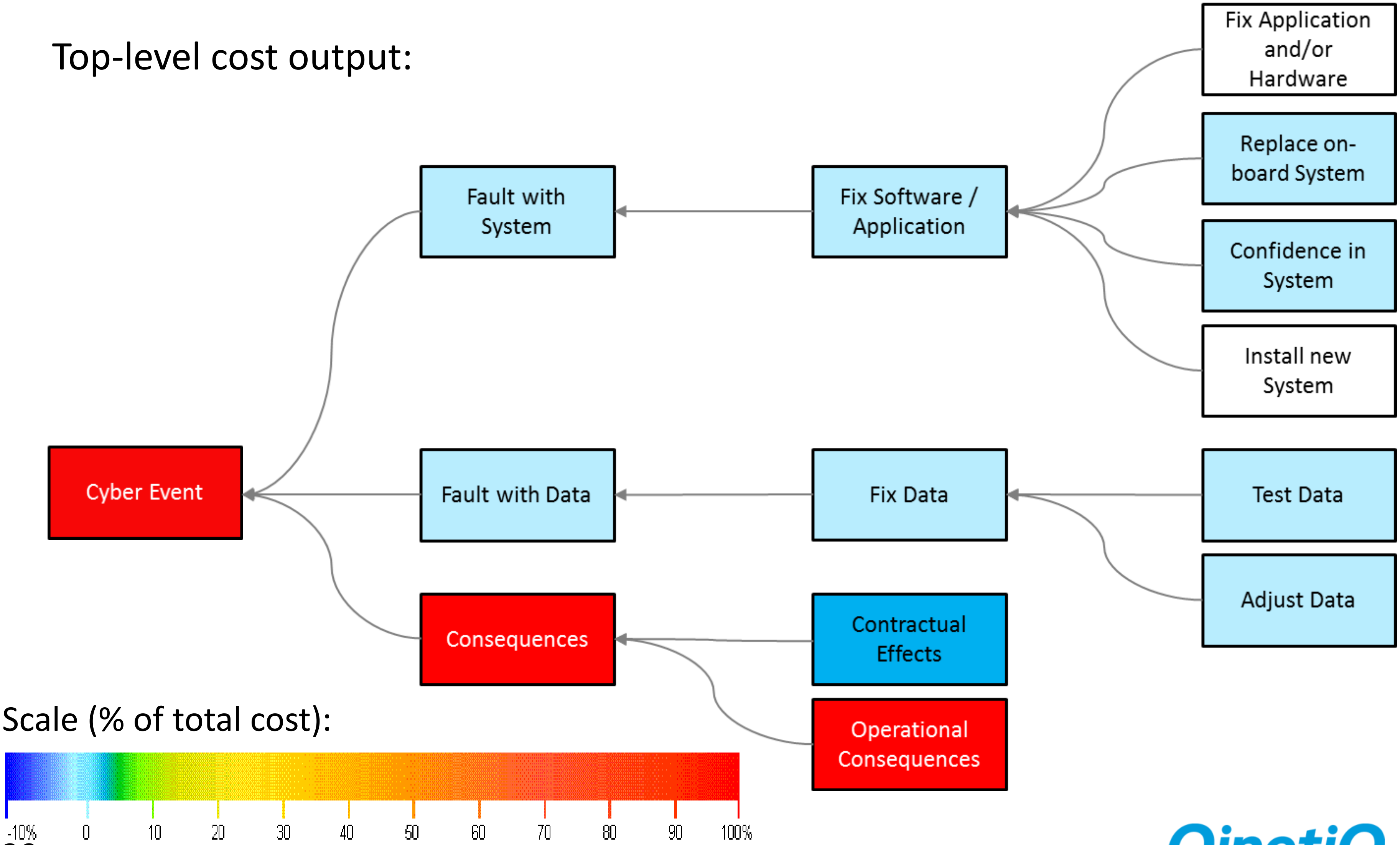
2. Attack detected, data corruption occurs.

This time the attack has caused a data corruption in the IT system.



2. Attack detected, data corruption occurs.

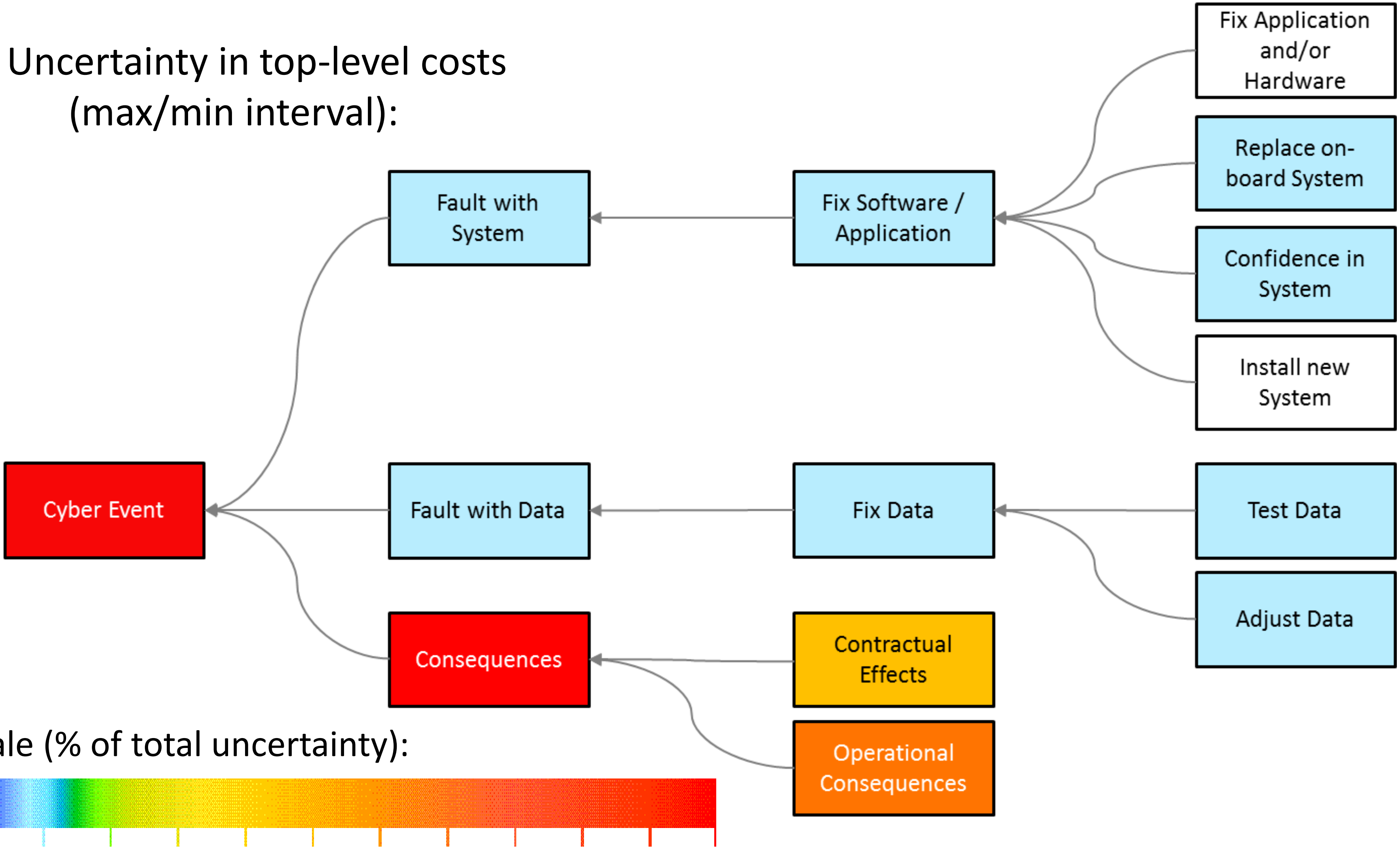
Top-level cost output:



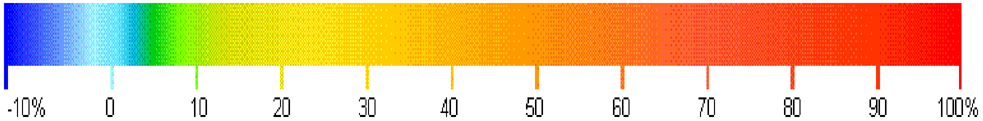
Scale (% of total cost):

2. Attack detected, data corruption occurs.

Uncertainty in top-level costs (max/min interval):

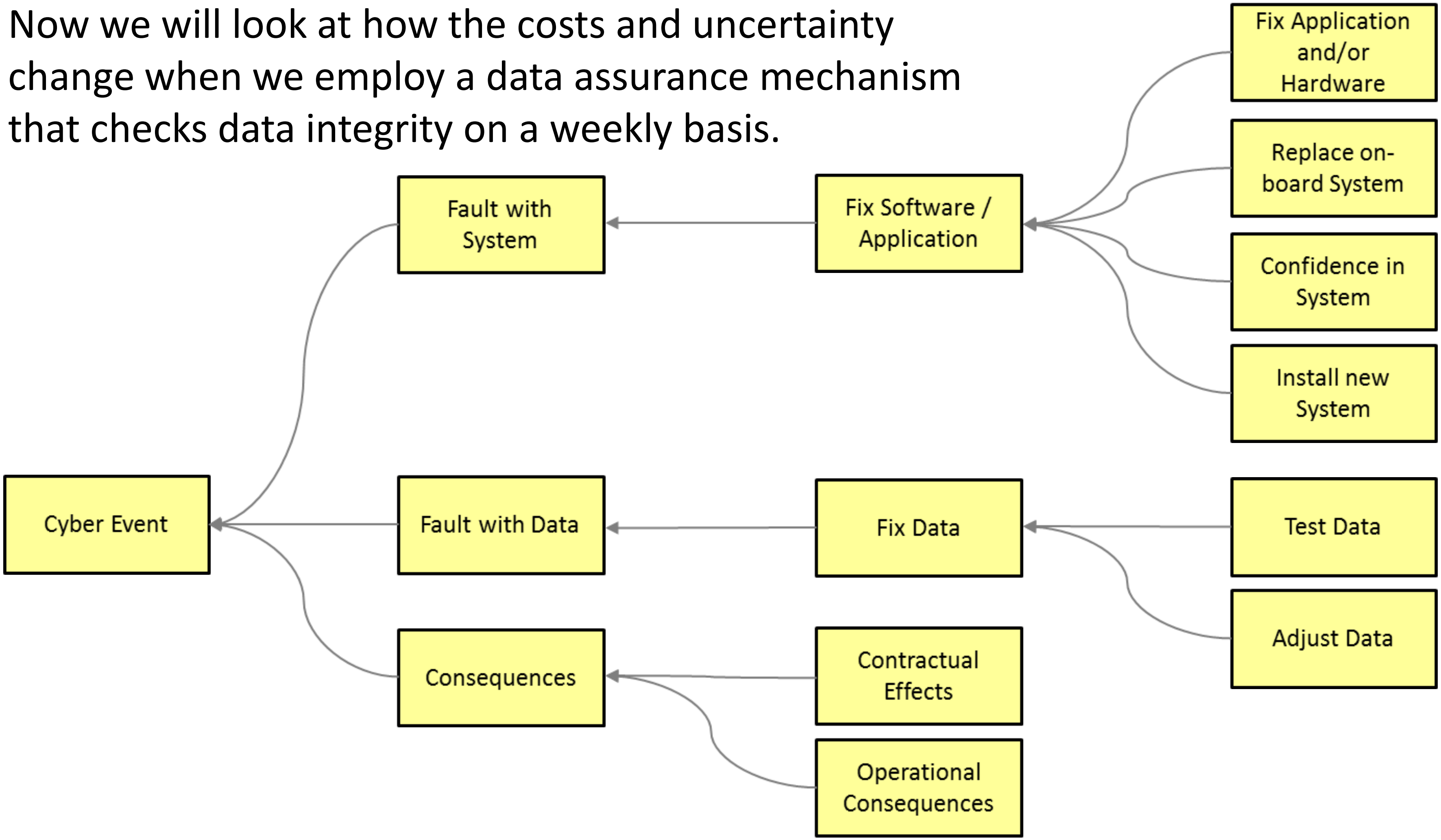


Scale (% of total uncertainty):



3. Mitigation: Data Integrity Assurance added

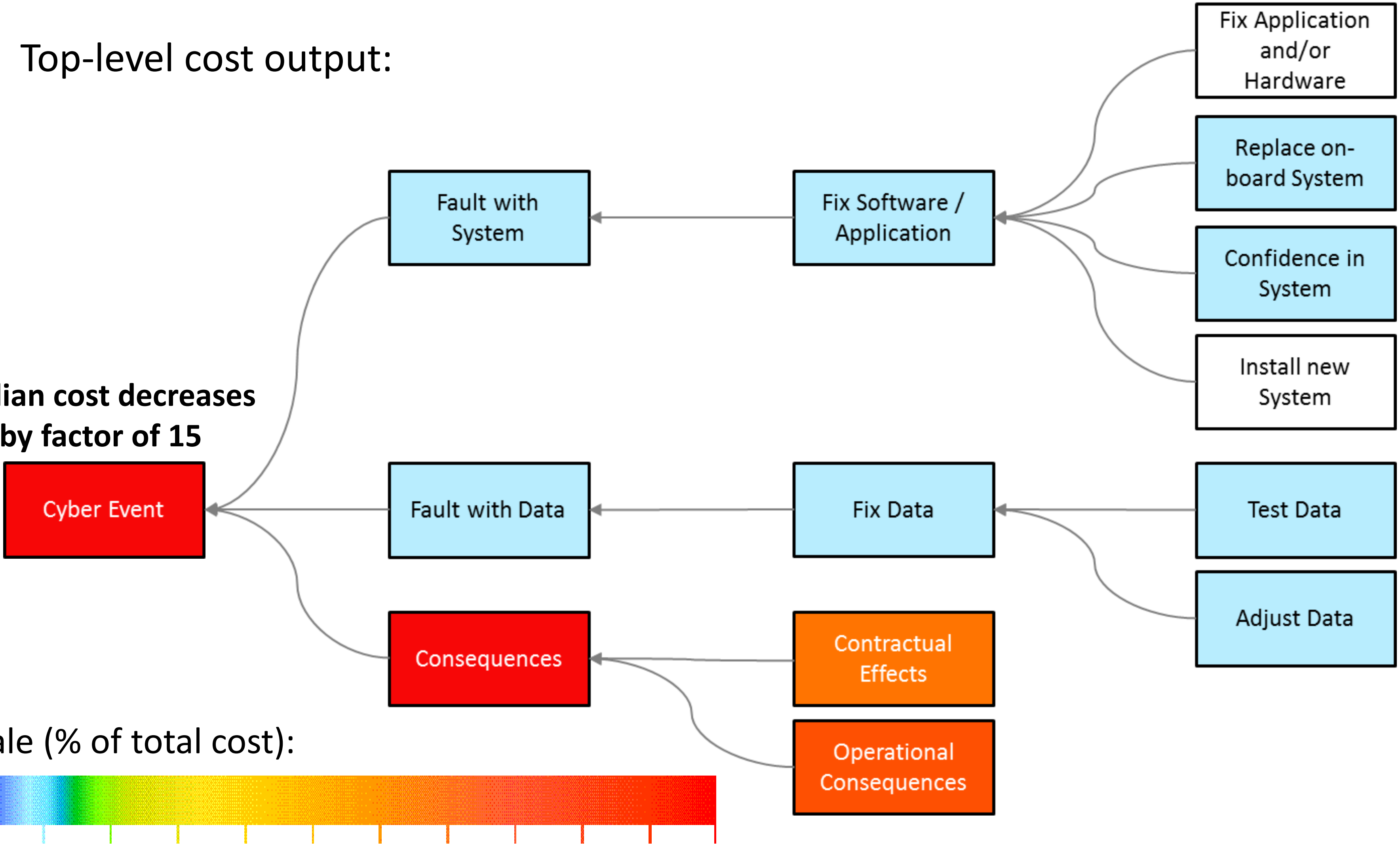
Now we will look at how the costs and uncertainty change when we employ a data assurance mechanism that checks data integrity on a weekly basis.



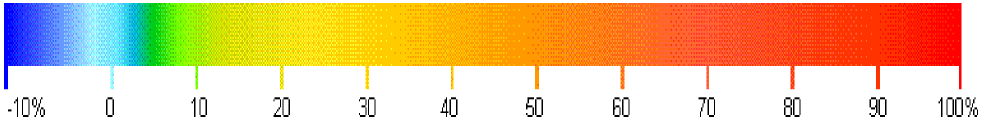
3. Mitigation: Data Integrity Assurance added

Top-level cost output:

Median cost decreases by factor of 15



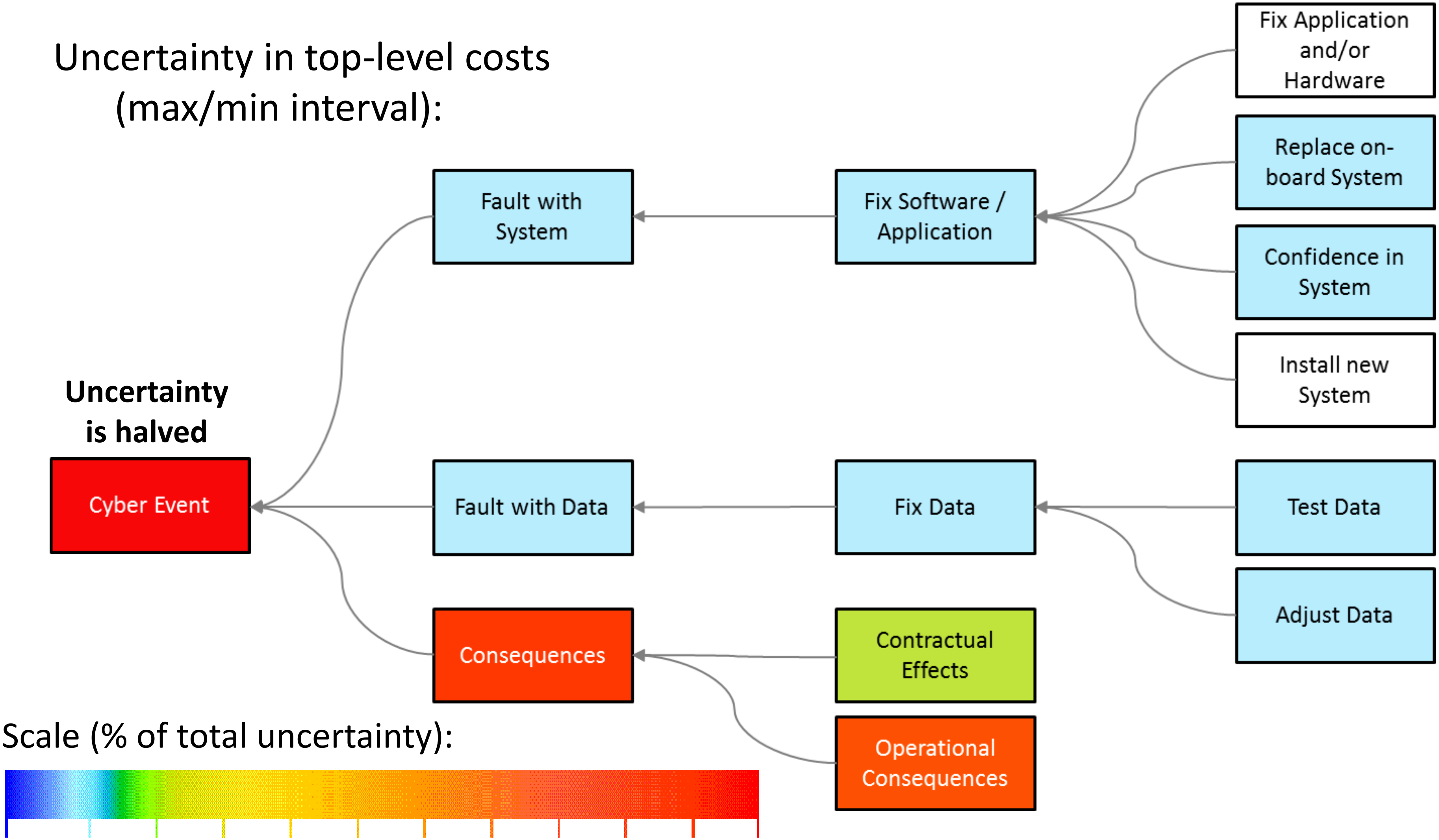
Scale (% of total cost):



3. Mitigation: Data Integrity Assurance added

Uncertainty in top-level costs (max/min interval):

Uncertainty is halved



Cyber Event

Fault with System

Fault with Data

Consequences

Fix Software / Application

Fix Data

Contractual Effects

Operational Consequences

Fix Application and/or Hardware

Replace on-board System

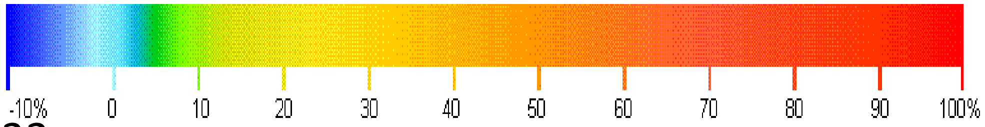
Confidence in System

Install new System

Test Data

Adjust Data

Scale (% of total uncertainty):



Contents

- Overview of EVC Technique
- EVC Study Analysis
- Summary

Three advantages of the EVC method

1. **Clearly identifies problem areas**
   - Node colouring allows identification of cost drivers
   - Uncertainty analysis highlights where further research is required
2. **Saves time and effort**
   - Diagrams and modules can be re-used
   - Only uses cost delta – no knowledge of base costs required
   - Inherent validation and audit trail
3. **Simplicity of presentation**
   - Cost, consequence and uncertainty displayed on a single diagram
   - Don’t need to be expert to interpret output.

ADBarwell@QinetiQ.com

www.QinetiQ.com

Publication Number:

QINETIQ/15/02544