Project Controls Expo – 16th Nov 2017
Emirates Stadium, London

Economic Value Chains - costing the impact of risk

About the speakers

Peter Tart

- Operational Analyst with 20 years experience primarily within Defence.
- Specialises in Balance of Investment, option assessment methods and benefits analysis.
- Development of bespoke cost capability trade methods.

Colin Sandall

- Operational Analyst with over 25 years' experience in Defence.
- Costing experience includes cost-benefit analysis on numerous projects across a range of different domains.
- Inventor of Economic Value Chains.

About the topic

Topic Outline

Unmitigated disruptive events have potentially catastrophic effects on businesses. Even where the aim of a cyber-attack is not economic, the project delays, cost of recovering capability and loss of reputation from such attacks can cripple organisations.

Many organisations do not understand the full scope and scale of potential recovery costs which makes it difficult to justify decisions relating to investment in cyber defences or improved project controls.

NHS WannaCry attack 12th May 2017

WannaCry was the largest cyber attack to affect the NHS

The attack led to disruption in at least 34% of trusts in England, although full extent unknown

The NHS was warned about the risks of cyber attacks a year before WannaCry

Five trusts had to divert patients to accident and emergency departments further away

Could have caused more disruption if it had not been stopped by a cyber researcher

Thousands of appointments and operations were cancelled

Organisations could have taken relatively simple action to protect themselves

The Department does not know how much the disruption to services cost the NHS

Project Controls EXPO

NAO's view on NHS WannaCry attack

Cost of action	**Organisations could have taken relatively simple action to protect themselves**
Cost of inaction	**The Department does not know how much the disruption to services cost the NHS**

EVC is a novel technique to aid calculation of the cost of inaction and the cost benefit of action

Cyber attack is an organisational risk

Risk sources

- Project inaction causes risk
  - Not having sufficient safeguards
  - Not implementing in a timely manner
- Project action causes risk
  - Withdrawal of fall backs
  - Introduction of new threat vectors
- External changes introduce risk

- **Cyber vulnerabilities occur at organisational level**

Cyber attack consequence and mitigation

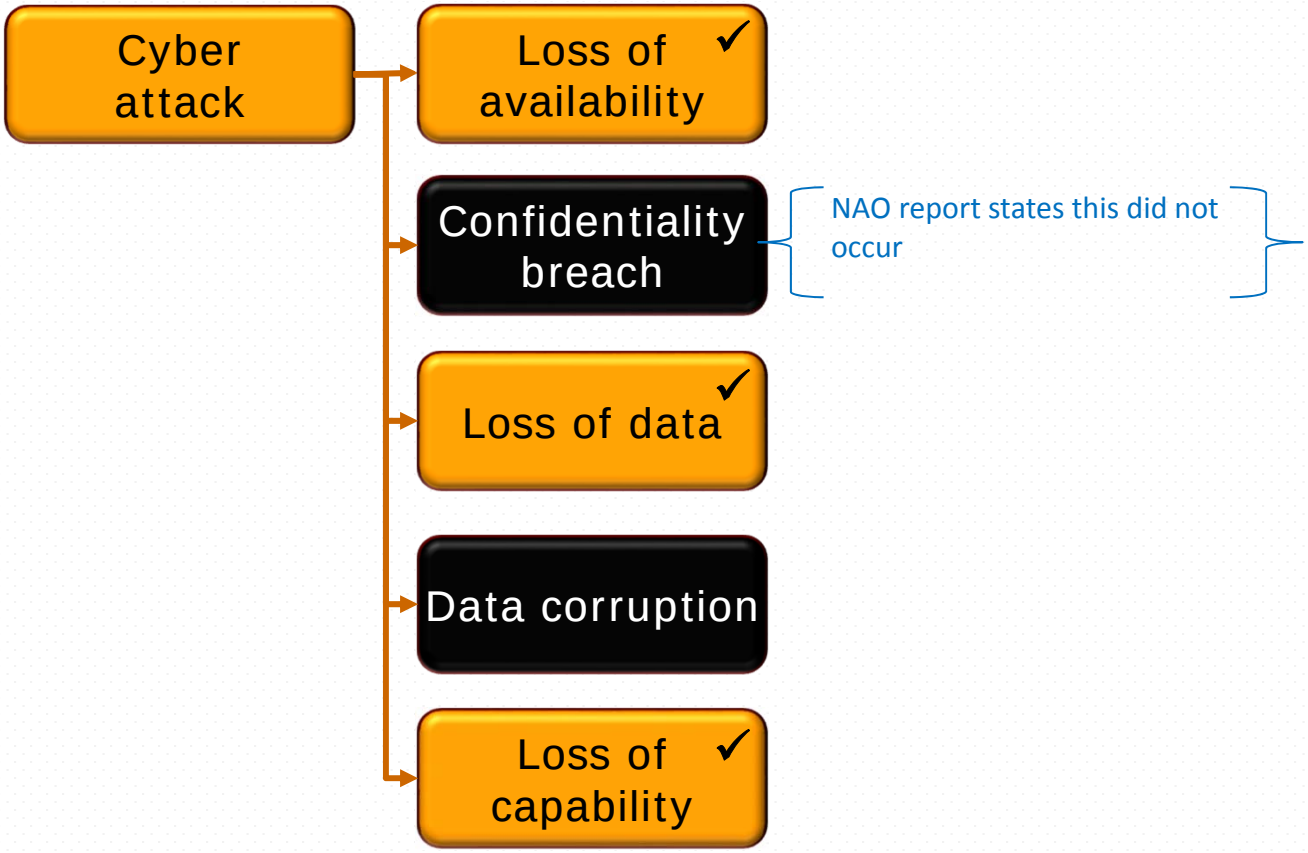
Quantifying the consequences

- A technique to identify and quantify effect on organisation
- History is illustrative – it isn't necessarily a true reflection of the risk
- The cost of identifying non-effects

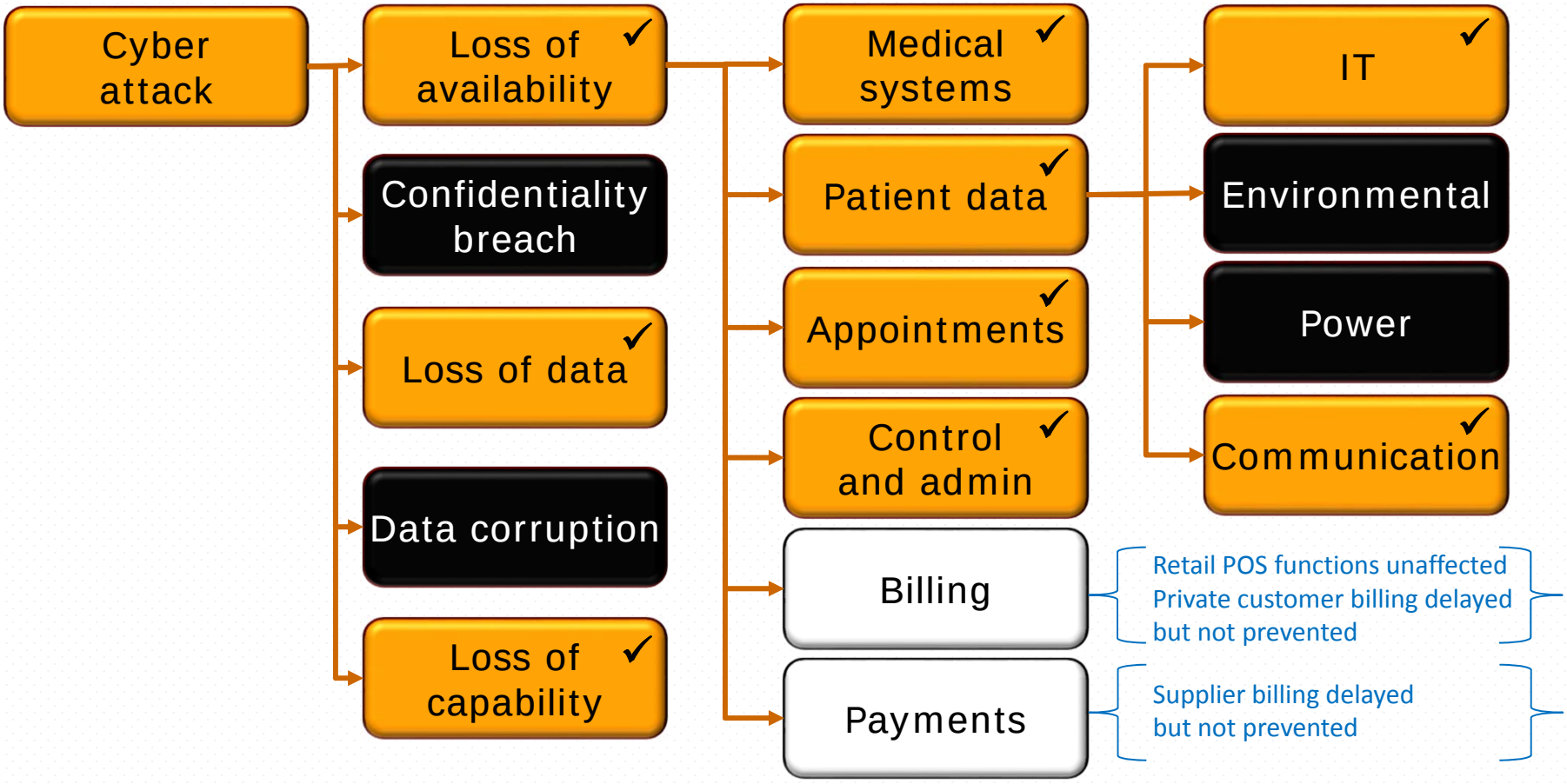
Mitigation options

- Quantify the cost effect of mitigation
- Ordering and prioritisation of options and risks
- Determining cost benefit of cost of action and cost of inaction

Economic Value Chains

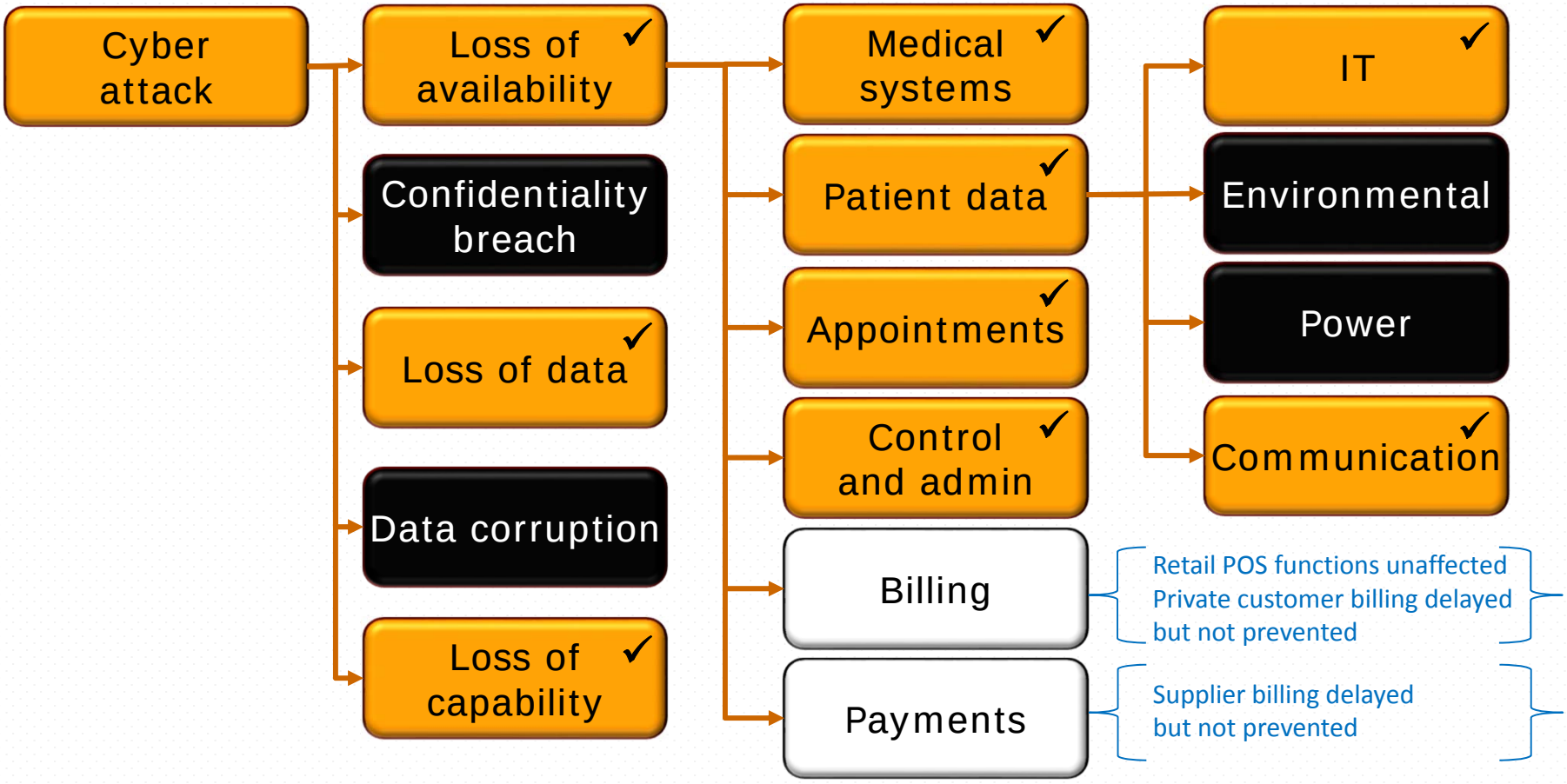


Economic Value Chains



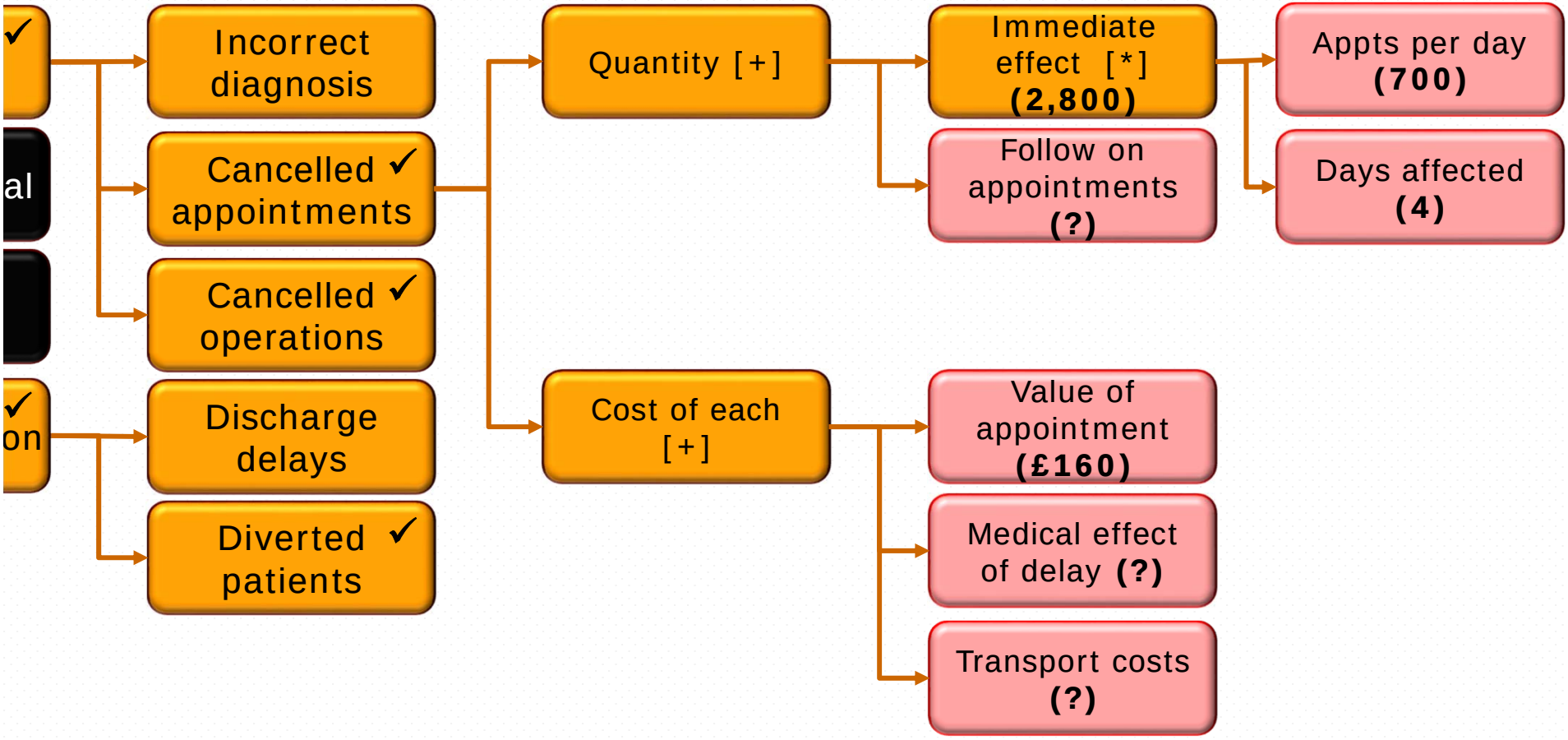
Project Controls EXPO

Economic Value Chains



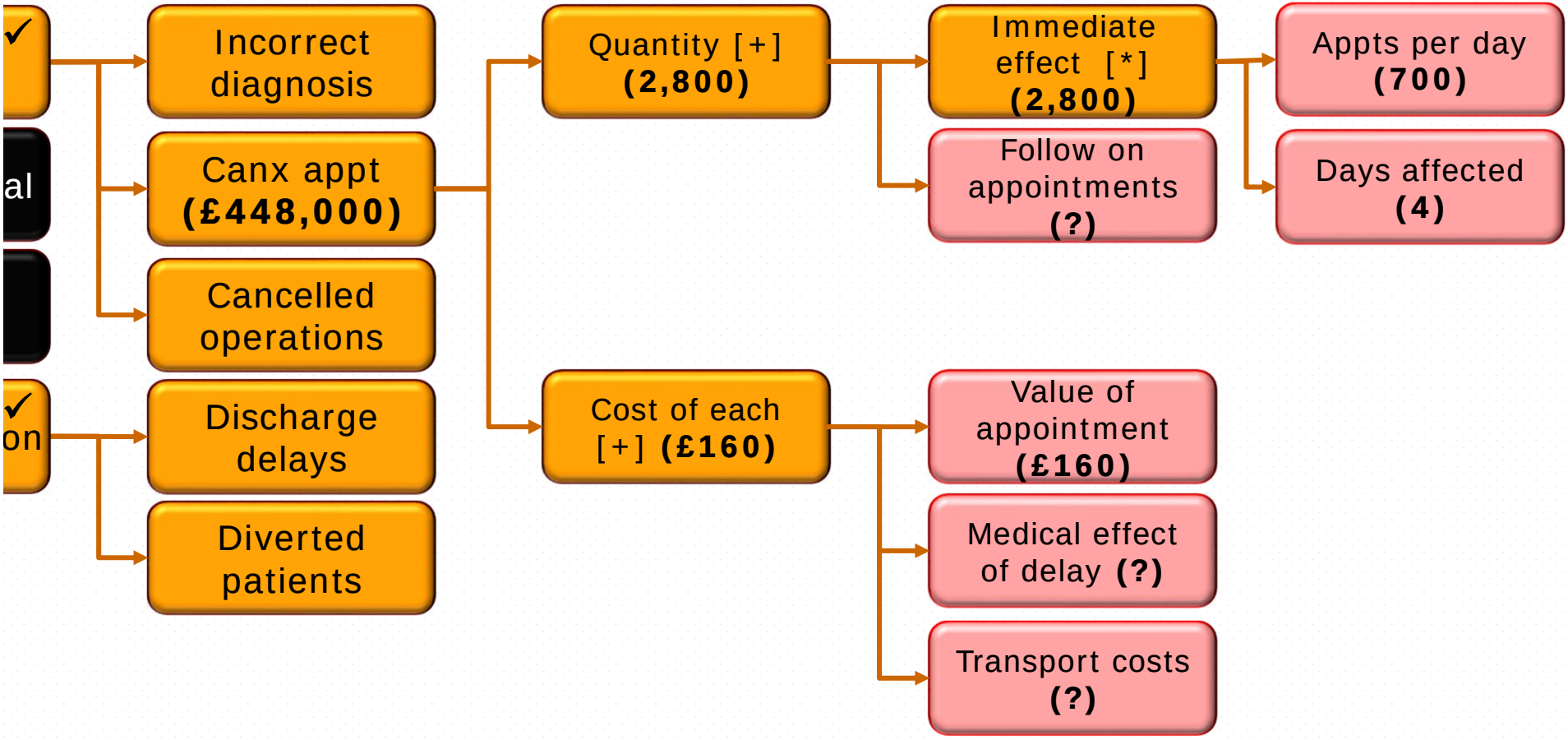
Project Controls EXPO

Economic Value Chains



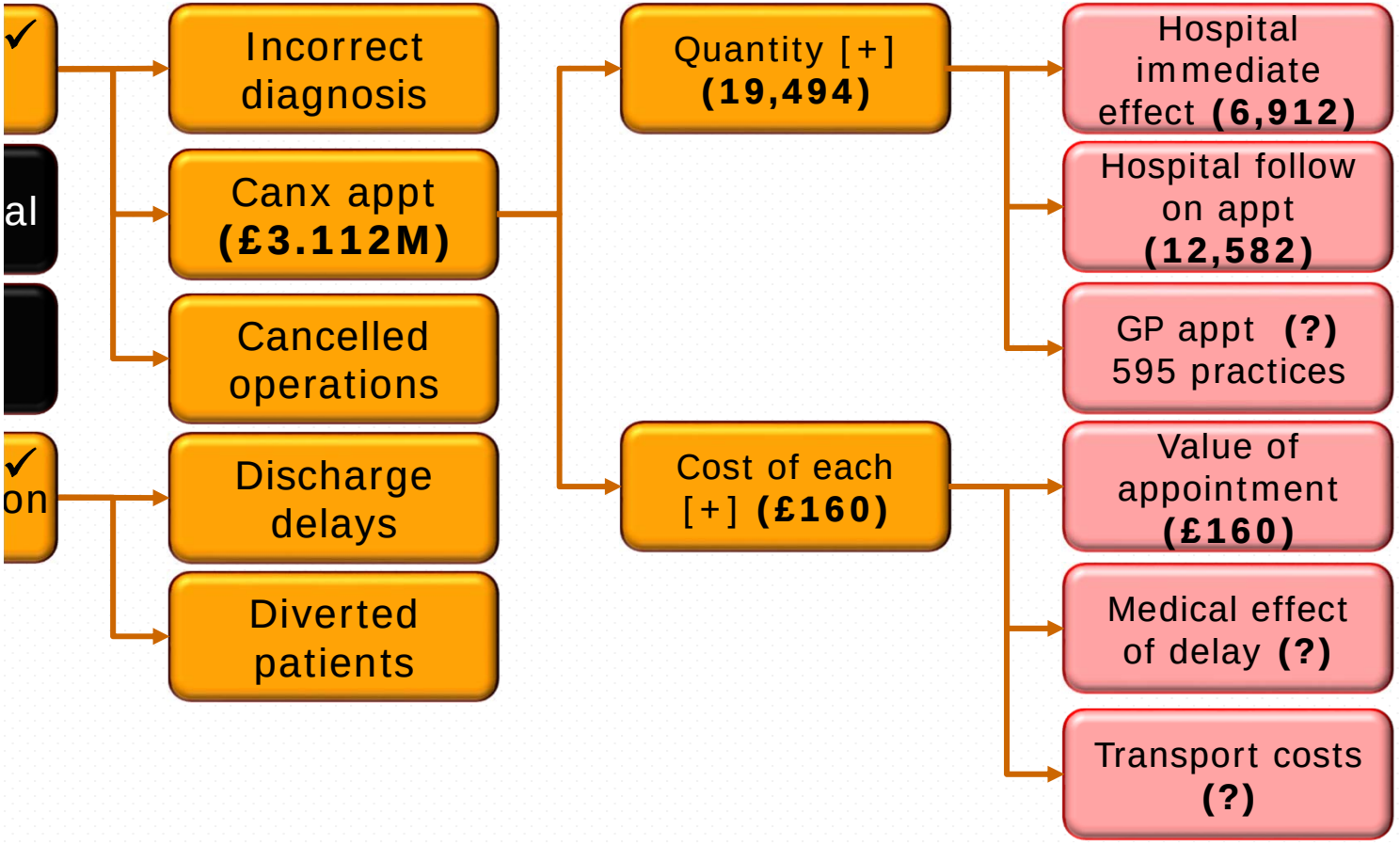
Project Controls EXPO

Economic Value Chains



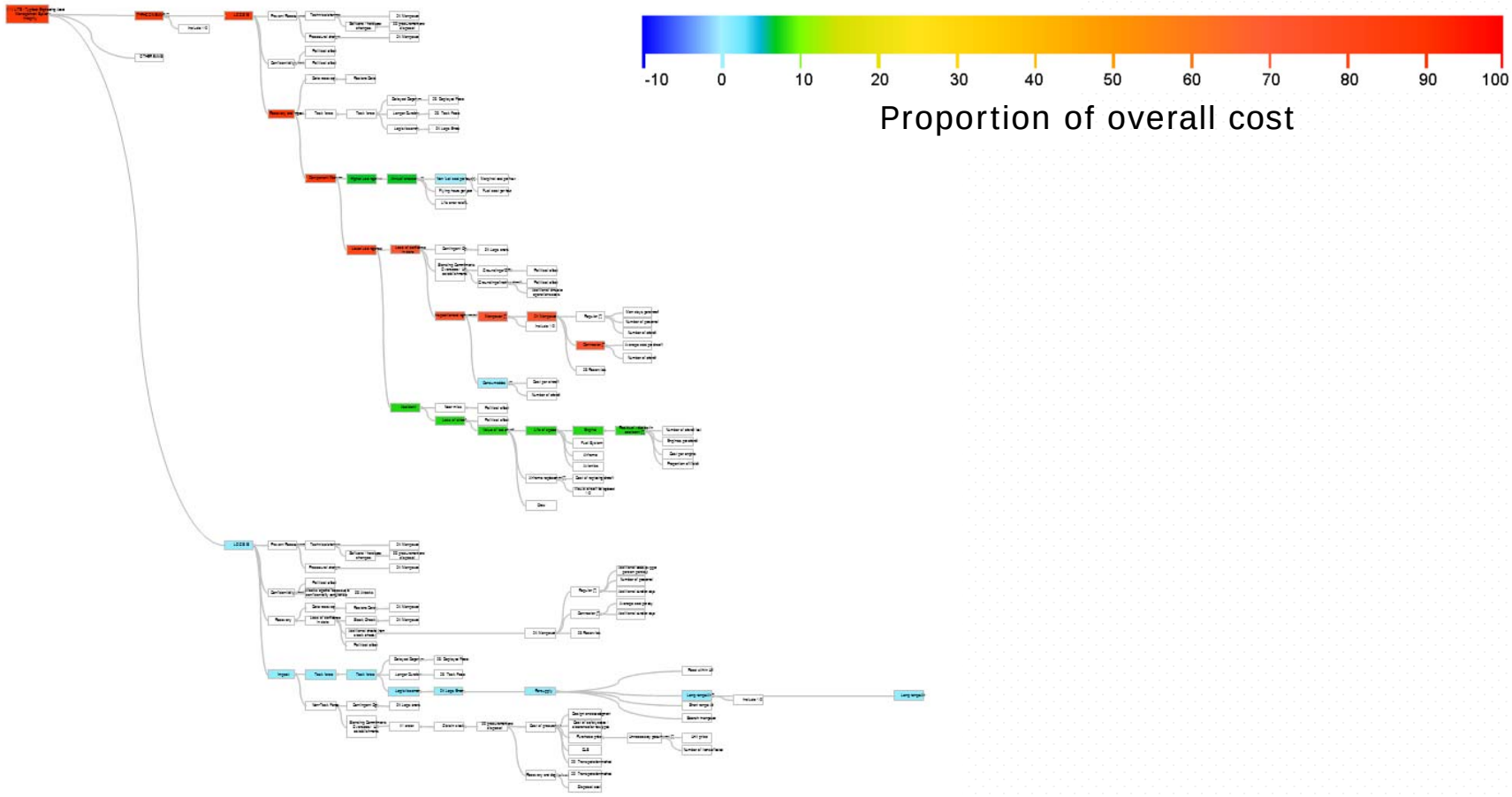
Project Controls EXPO

Economic Value Chains



Project Controls EXPO

Economic Value Chains



Project Controls EXPO

Economic Value Chains

EVC does not attempt to cost everything

- Only consider what changes as a result of an event
- Only cost where costs change
- Explicitly identify what is excluded (black nodes) with explanation
- Explicitly identify zero cost (white nodes) with explanation

The EVC tree is the mechanism for

- Capturing the causality chain
- Explaining the structure
- Gaining stakeholder buy-in
- Defining the calculations – the diagram is the model
- Explaining the results

Economic Value Chains

Mitigation options

- Quantify the cost effect of mitigation
  - Unplug diagnostic equipment: reduction in infection, but increase in downtime
  - Disconnect external firewall: reduction in infection, but increase in downtime and knock-on effect to non-infected trusts
  - Reduction in downtime by reduced infection
  - Reduction in effect by detection / remediation procedures and fall-back
- Ordering and prioritisation of options and risks
- Determining cost and benefit of action vs the cost of inaction

Economic Value Chains

Caution ! - History is only illustrative

- WannaCry first detection Friday 12th May late morning.
- Blocked (by luck) evening of 12th.
- WannaCry very obvious, not all cyber attacks are.
- Not targeted at NHS.
- Infection occurred Friday, giving trusts times to react before Monday.

Trusts didn't react to previous events

- Same trust which was infected in October 2016 infected by WannaCry.
- Patch issued by Microsoft March 2017.
- NHS Digital alerts 17th March and 28th April to install patch.

Economic Value Chains

QinetiQ's EVC technique is

- A thorough bottom-up investigation of risk and cost
- Guided by the past, but not mislead by it
- Transparent, visual and easy to comprehend
- Quick to use, easy to extend detail as required
- Capable of capturing organisation / enterprise level risks
- Capable of calculating the effect of individual projects on these risks
- Capable of correctly evaluating response and non-response to events
- Provides evidence for decision making

Economic Value Chains

Questions ?