Cambridge Judge Business School

Centre for Risk Studies 7th Risk Summit Research Showcase

Developing Scenarios for Managing Cyber Catastrophe Risk

Éireann Leverett

Senior Risk Researcher, Cambridge Centre for Risk Studies

20 June 2016
Cambridge, UK

Centre for
Risk Studies

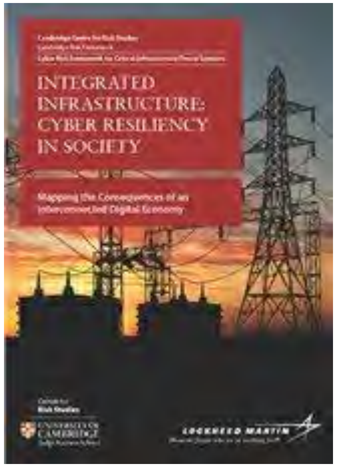
UNIVERSITY OF
CAMBRIDGE
Judge Business School

Business Blackout

- The Cambridge Centre for Risk Studies asked me what a catastrophic cyber attack would look like
- So we wrote one and then quantified the cost to the US economy of an extreme case
- We used the Lawton damage function to calculate direct costs
- We used Oxford Economics Model to calculate macroeonomic costs

Resilience in the UK

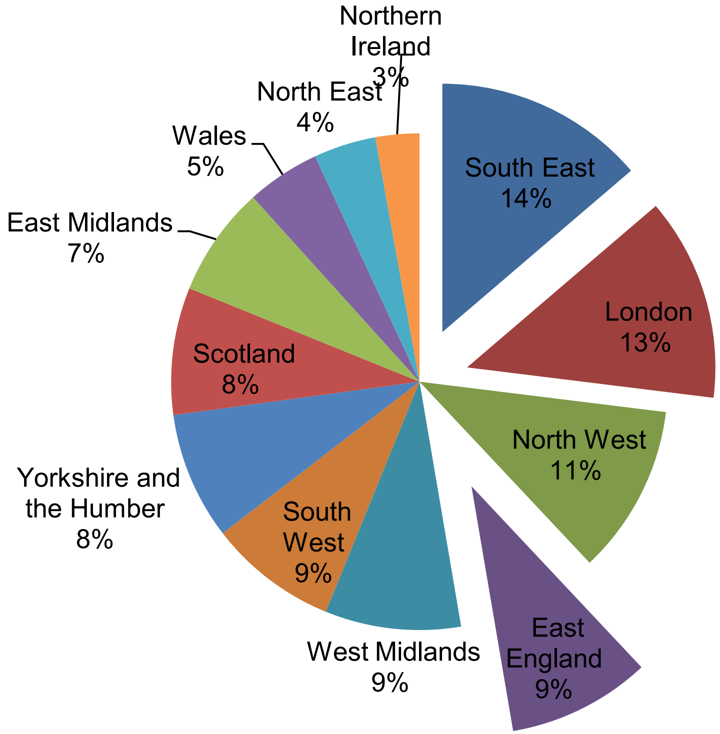
- What about a cyber attack on the distribution grid?
  - Our report is just out, and details the cost
  - We quantify the impact on GDP
  - We estimate dependencies of other critical infrastructures
  - We look at direct and indirect costs
  - And the disruption of transport networks
    - Rail disrupted up into Scotland
  - The effects of a power outage ripple into neighbouring areas, and over five years


INTEGRATED INFRASTRUCTURE: CYBER RESILIENCY IN SOCIETY
Mapping the Consequences of an Interconnected Digital Economy
Centre for Risk Studies
UNIVERSITY OF CAMBRIDGE
LOCKHEED MARTIN

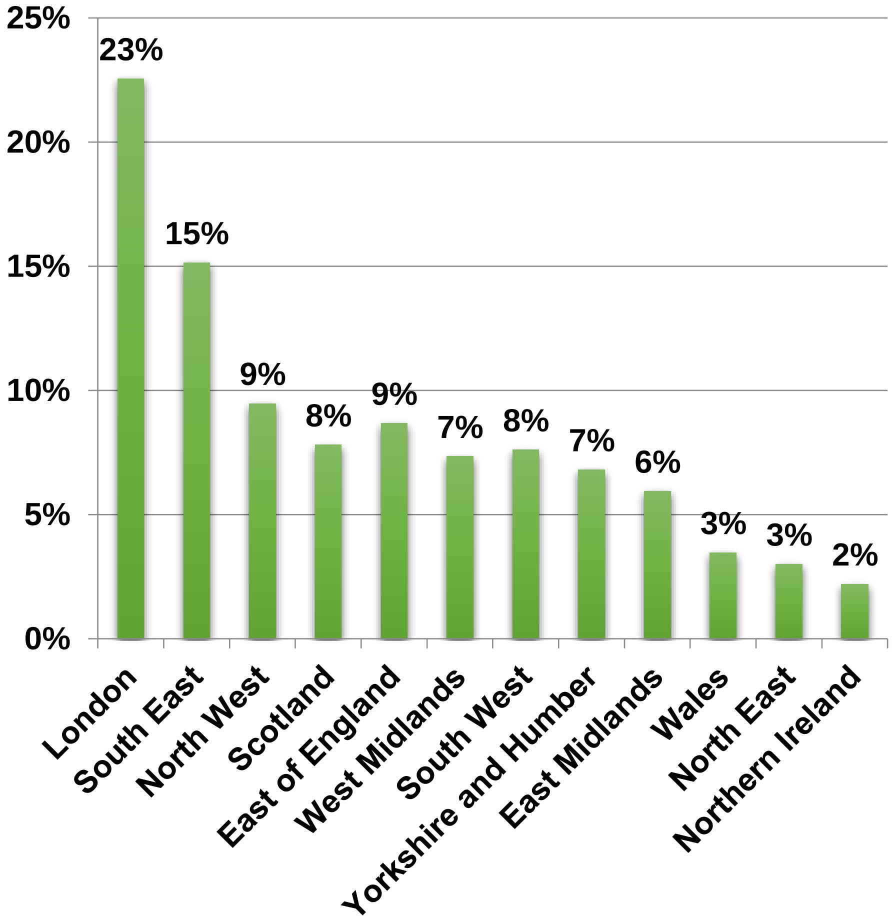
Target Location

The South East, London and East of England selected as target locations

Population share (%)



Total GVA by Region, 2013 as %



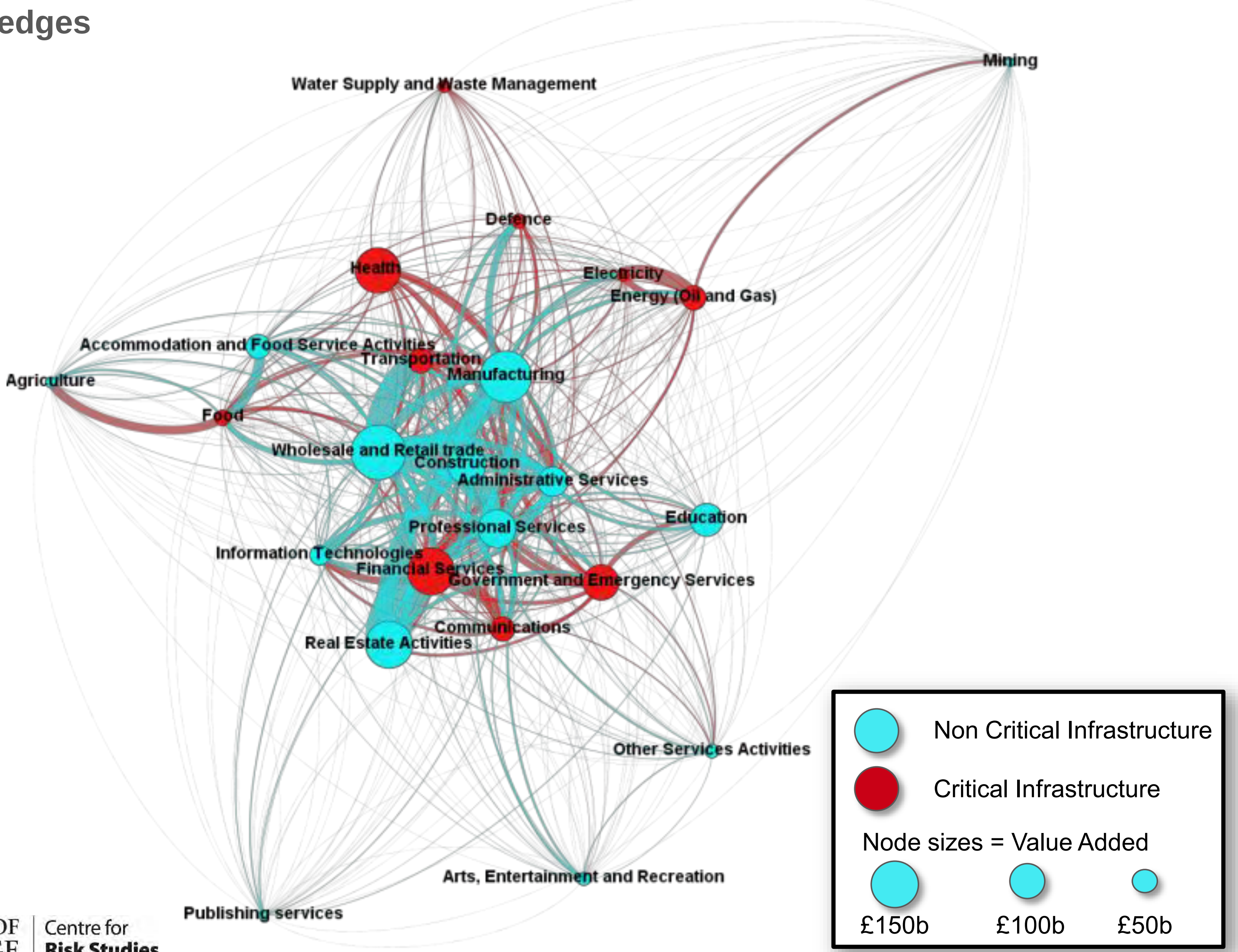
***GVA = gross value added, GVA is GDP excluding taxes and subsidies on production**

Source:

1. 2013 ONS population estimates. http://www.ons.gov.uk/ons/taxonomy/index.html?nscl=Population#tab-data-tables
2. Harari, Danei. Regional and Local Economic Growth Statistics. House of Commons Library. Dec 2014.

Network Linkages of UK Economic Sectors

All network edges

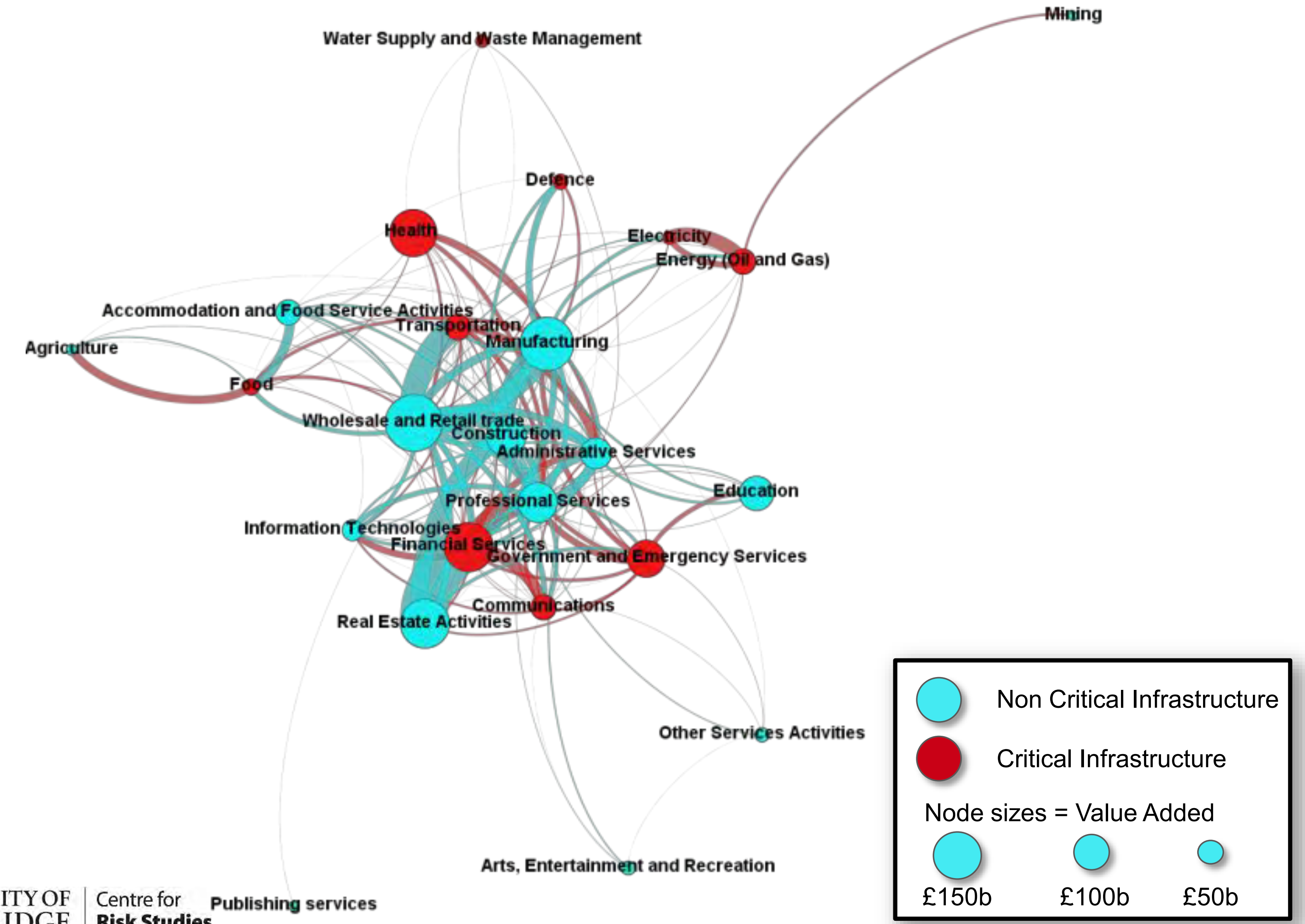


UNIVERSITY OF CAMBRIDGE Judge Business School | Centre for Risk Studies

Data Source: UK IO Tables, revised 2014

Key Network Linkages of UK Economic Sectors

All edges > £1 billion

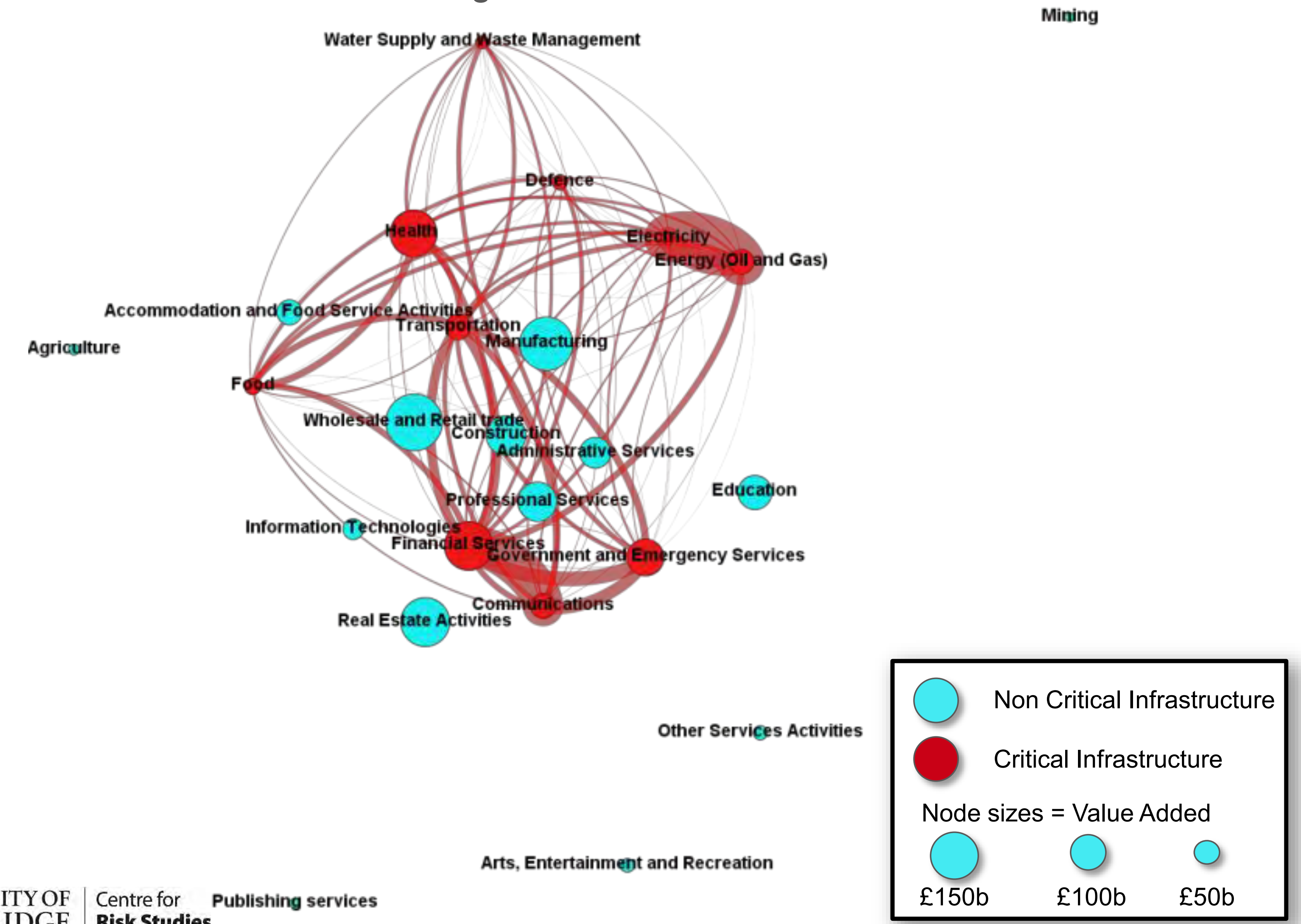


UNIVERSITY OF CAMBRIDGE Judge Business School | Centre for Risk Studies

Data Source: UK IO Tables, revised 2014

Network Linkages of UK Critical Infrastructure Sectors

Only infrastructure to infrastructure edges

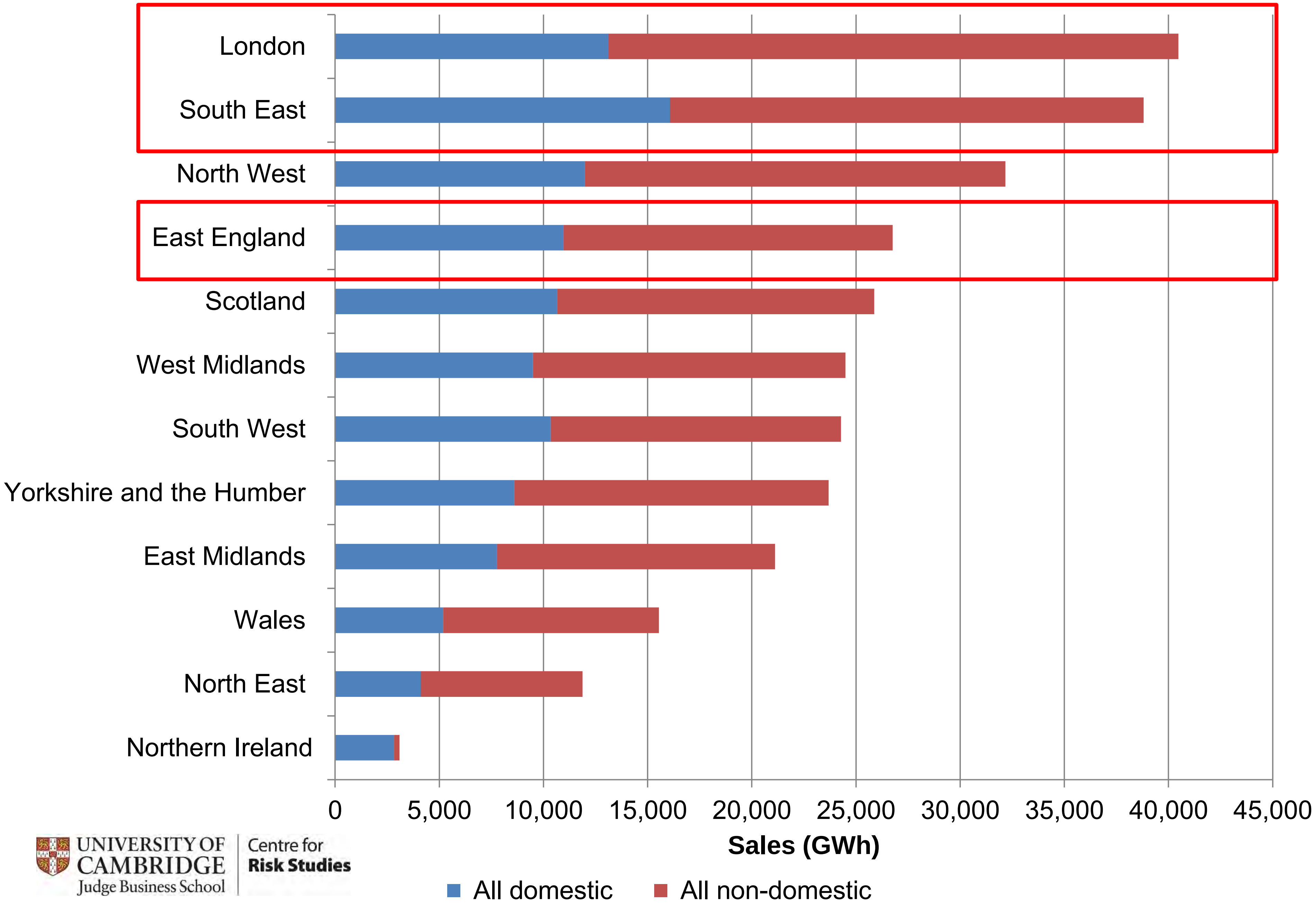


UNIVERSITY OF CAMBRIDGE
Judge Business School

Centre for
Risk Studies

Data Source: UK IO Tables, revised 2014

Regional Electricity Consumption



UNIVERSITY OF CAMBRIDGE
Judge Business School

Centre for
Risk Studies

Population Affected

Region	Population	Population share (%)	S1 coverage	S2 coverage	X1 coverage
South East	8,873,800	13.74%	2,519,228	3,323,551	3,949,286
London	8,538,700	13.22%	3,530,536	4,279,823	4,585,807
North West	7,133,000	11.04%	0	0	0
East England	6,018,400	9.32%	2,641,328	3,574,195	4,374,594
West Midlands	5,713,300	8.84%	0	0	0
South West	5,423,300	8.40%	0	0	0
Yorkshire and the Humber	5,360,000	8.30%	0	0	0
Scotland	5,347,600	8.28%	0	0	0
East Midlands	4,637,400	7.18%	0	0	0
Wales	3,092,000	4.79%	0	0	0
North East	2,618,700	4.05%	0	0	0
Northern Ireland	1,840,500	2.85%	0	0	0

	S1	S2	X1
Population affected (%)	13.45%	17.30%	19.99%
Rolling blackouts	6.73%	8.65%	9.99%

Making Your Own Stress Tests

- Choose a particular cyber attack
  - One that concerns you
  - Quantification is therapeutic
- Assume it happened
  - then work backwards to figure out how it could
- Assume things failed
  - Controls didn't work
  - That happens in reality
  - Identify why it might
- Now quantify the cost to your company
- Then quantify the cost to society
  - (if you dare)
  - Discuss what the company should pay
  - Discuss what gov't should pay
    - Before for proactive
    - After for reactive
- Much more could be shared across multiple companies than IS!

How to Choose a Disaster

- Don’t choose attacks that are common
  - You already know what they cost
- Choose weird things that are plausible
  - Real world disasters ARE weird
- Guiding principles:
  - Destabilise the business
  - Lose 1/3 of a yearly revenue
  - Force multi-organisational collaboration and response
- This is not to be a scare monger, it serves to help you identify all the controls, existing and possible.
- It focuses hearts and minds to work on an existential threat.

Quantify the Losses

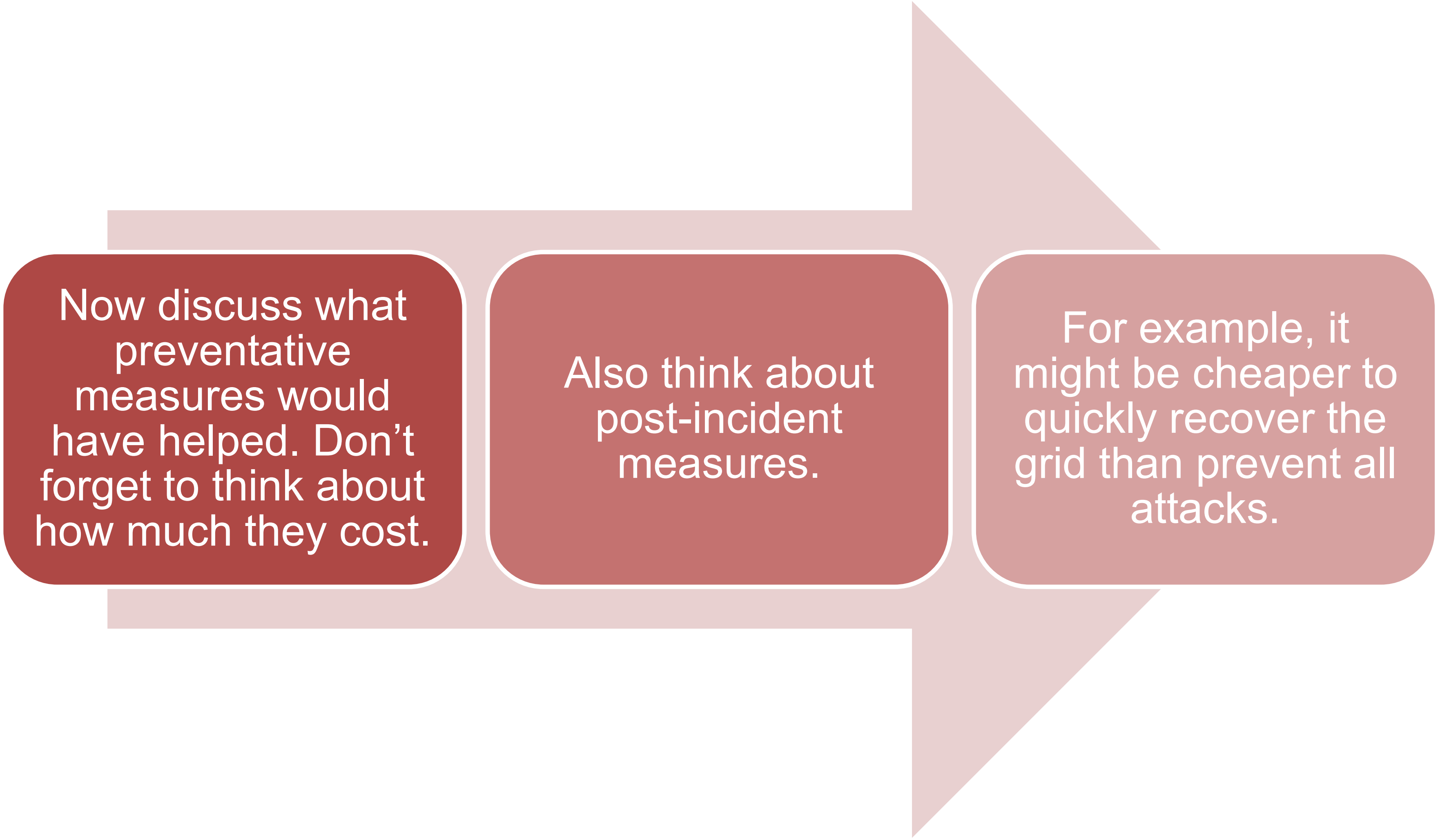
Think about:

- Lost revenues
- Incident Cost
- Forensic Cost
- Potential liability
- Legal Costs
- Regulatory Costs
- Hidden Costs

Get experts in your organisation to estimate

- When they don't agree
- That's where you write scenario variants
- The variants contain the quantified disagreement
- This provides sensitivity testing:
  - Where uncertainty is greatest
  - Drives Expert engagement
  - Documents the debate

Discuss Mitigations

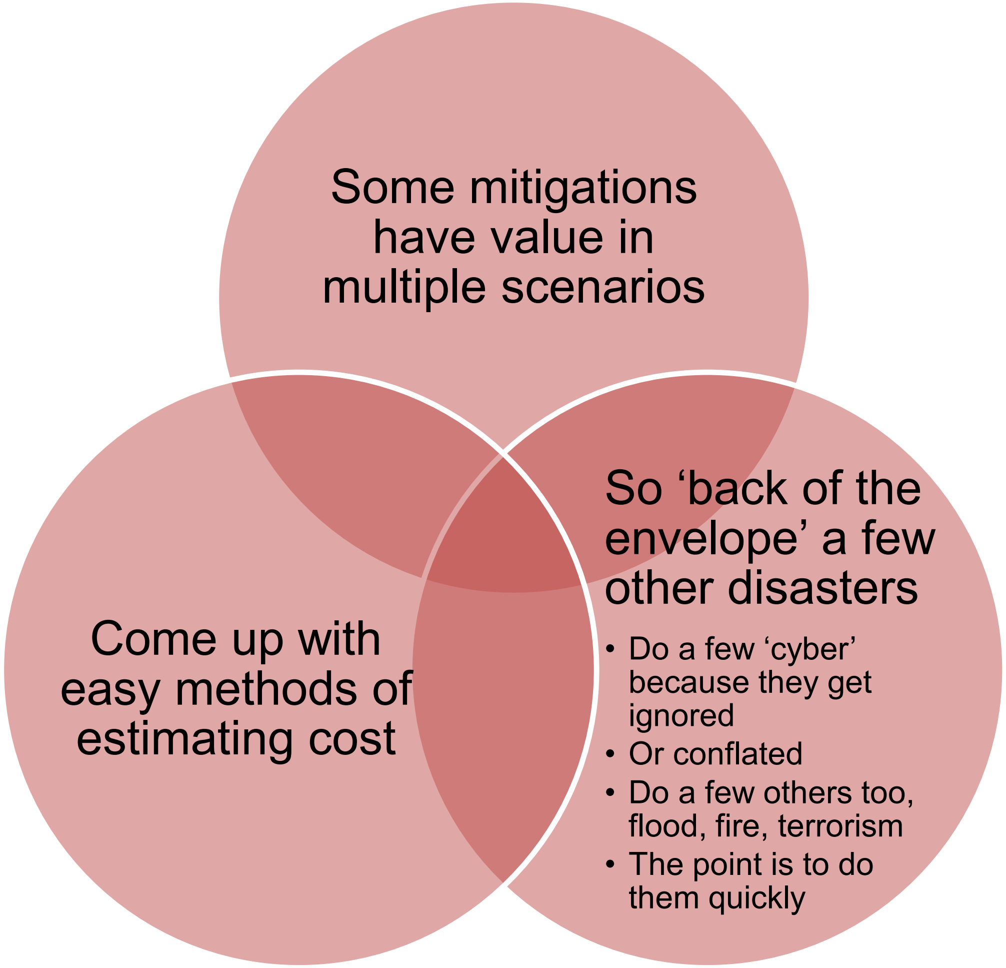


Now discuss what preventative measures would have helped. Don’t forget to think about how much they cost.

Also think about post-incident measures.

For example, it might be cheaper to quickly recover the grid than prevent all attacks.

Invent a Few More Disasters



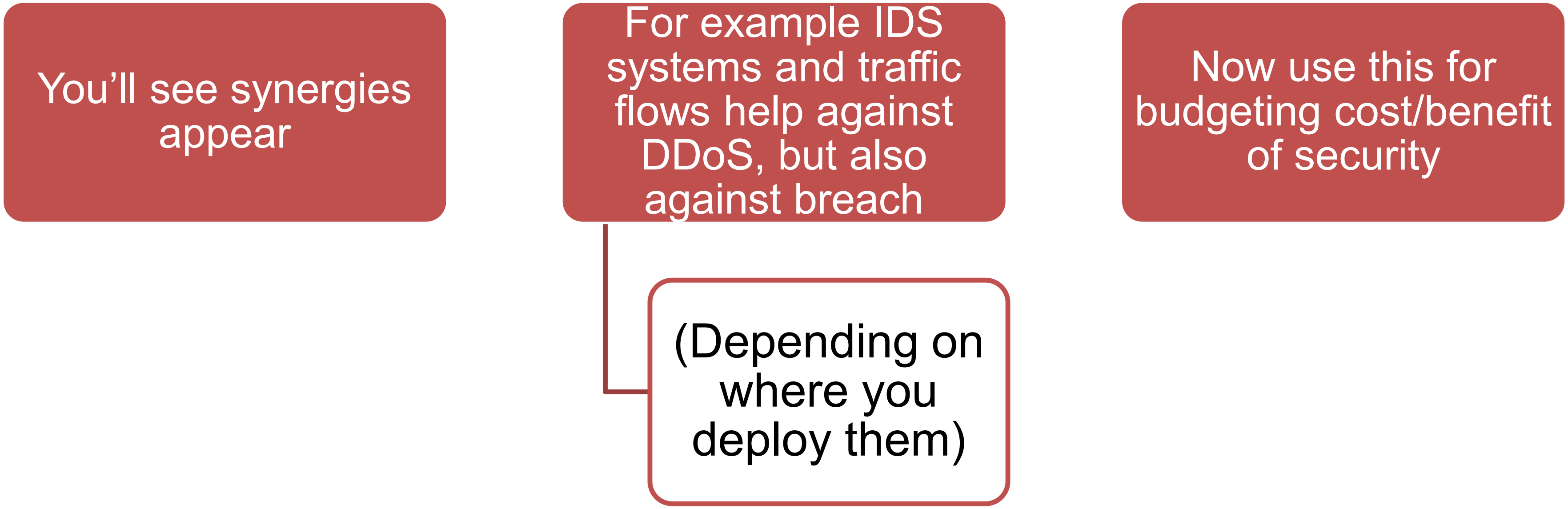
Some mitigations have value in multiple scenarios

Come up with easy methods of estimating cost

So ‘back of the envelope’ a few other disasters

- Do a few ‘cyber’ because they get ignored
- Or conflated
- Do a few others too, flood, fire, terrorism
- The point is to do them quickly

See Which Mitigations Cross Disasters



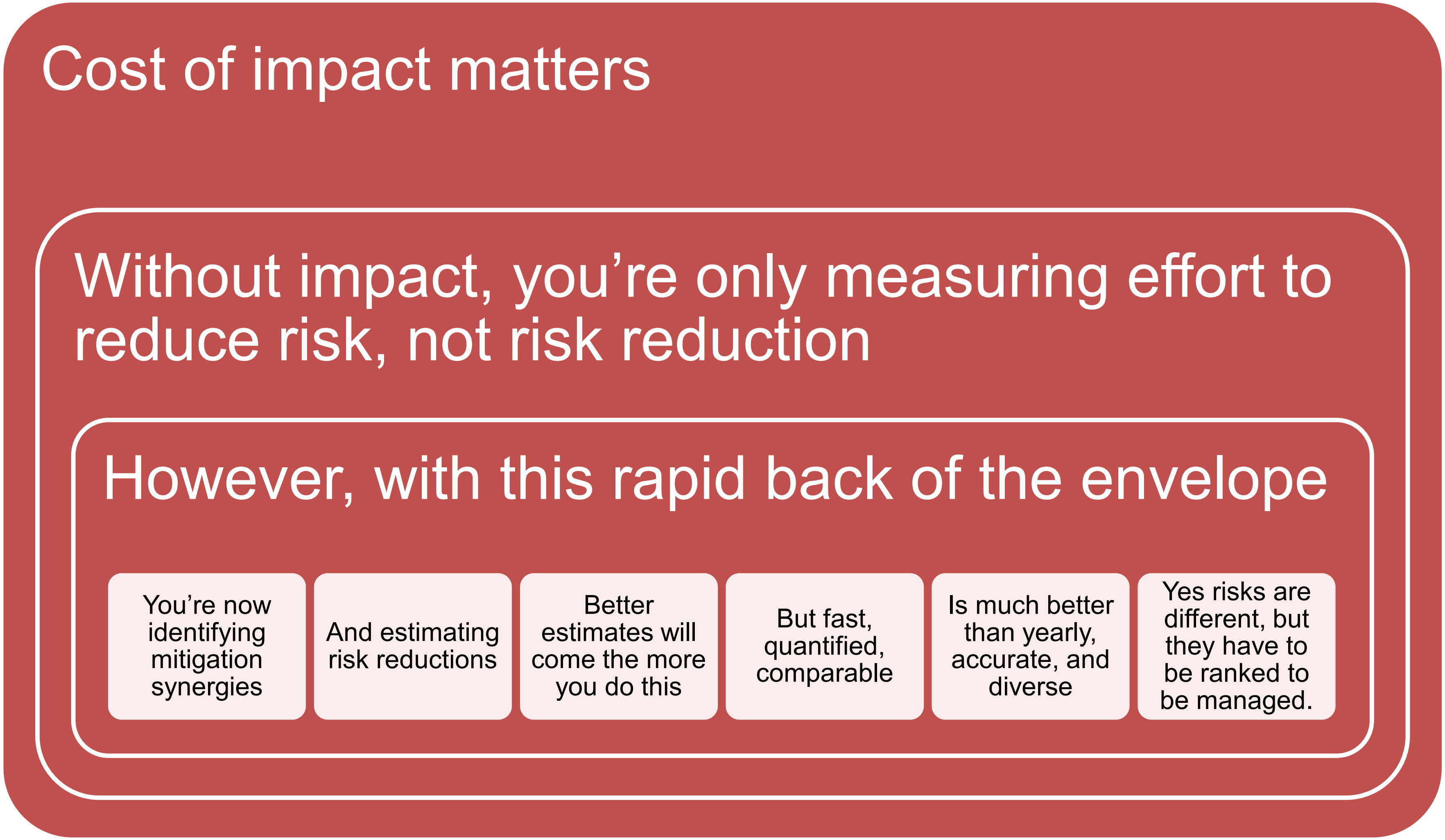
You'll see synergies appear

For example IDS systems and traffic flows help against DDoS, but also against breach

(Depending on where you deploy them)

Now use this for budgeting cost/benefit of security

Fund the Work that Helps All/Most Situations



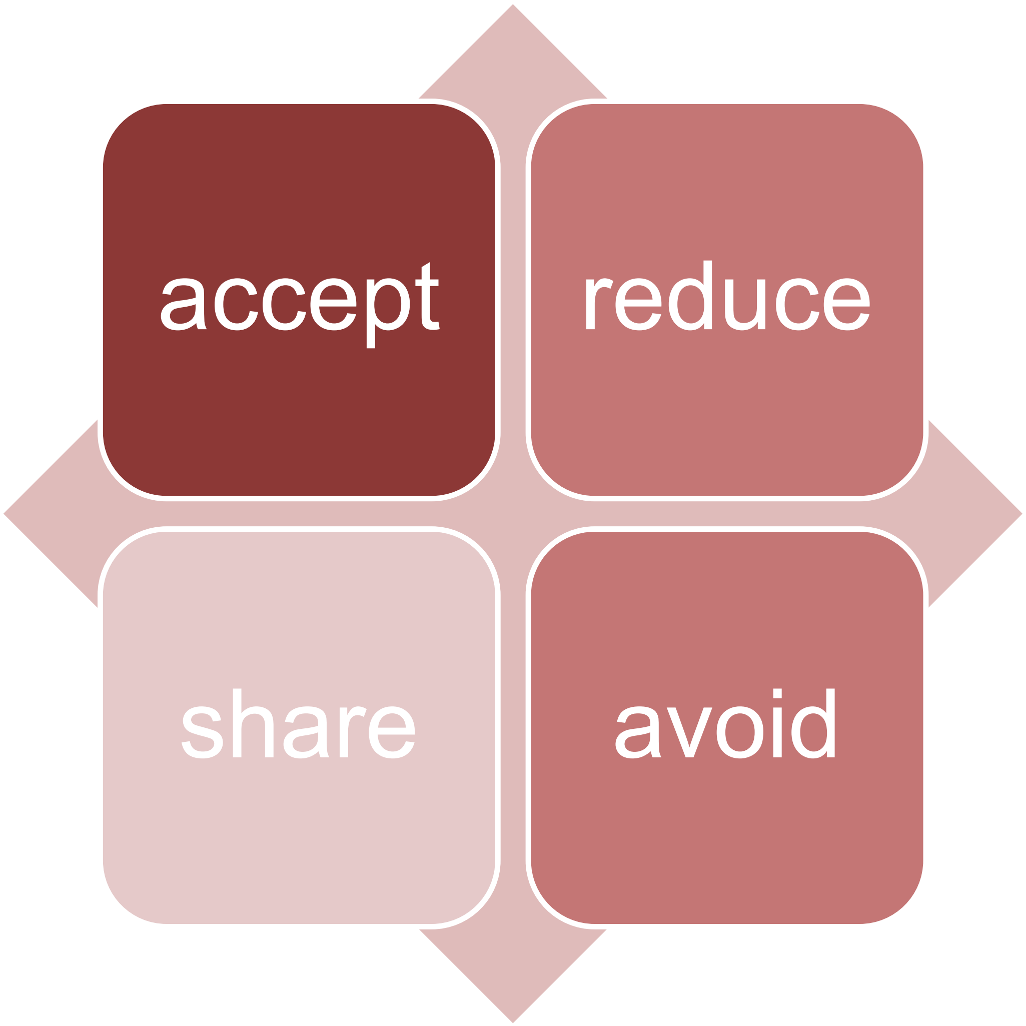
Cost of impact matters

Without impact, you’re only measuring effort to reduce risk, not risk reduction

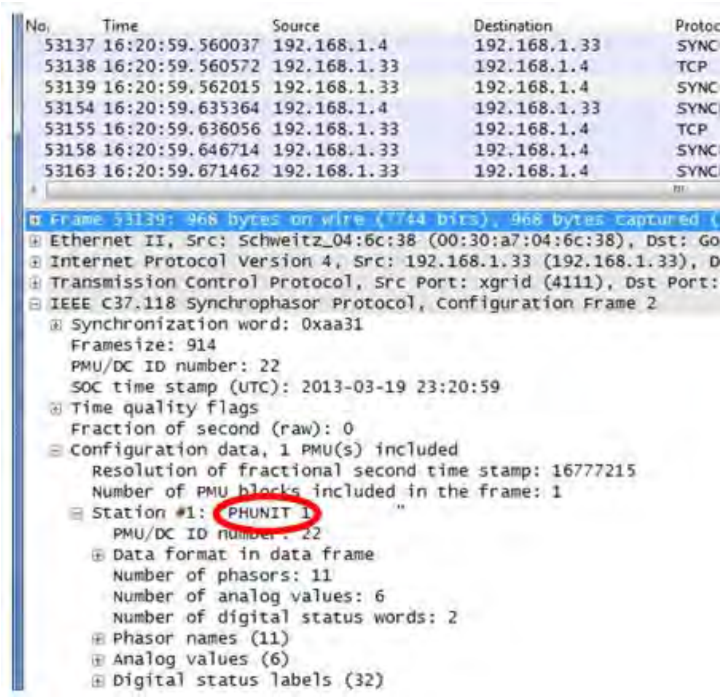
However, with this rapid back of the envelope

- You’re now identifying mitigation synergies
- And estimating risk reductions
- Better estimates will come the more you do this
- But fast, quantified, comparable
- Is much better than yearly, accurate, and diverse
- Yes risks are different, but they have to be ranked to be managed.

Now We Can Manage Our Cyber Risks



Too much acceptance, a little reduction, a pinch of avoidance, and hardly any sharing.



```
No.   Time              Source          Destination      Protoc
  53137 16:20:59.560037 192.168.1.4     192.168.1.33     SYNC
  53138 16:20:59.560572 192.168.1.33    192.168.1.4      TCP
  53139 16:20:59.562015 192.168.1.33    192.168.1.4      SYNC
  53154 16:20:59.635364 192.168.1.4     192.168.1.33     SYNC
  53155 16:20:59.636056 192.168.1.33    192.168.1.4      TCP
  53158 16:20:59.646714 192.168.1.33    192.168.1.4      SYNC
  53163 16:20:59.671462 192.168.1.33    192.168.1.4      SYNC

⊞ Frame 53139: 968 bytes on wire (7744 bits), 968 bytes captured (
⊞ Ethernet II, Src: Schweitz_04:6c:38 (00:30:a7:04:6c:38), Dst: Go
⊞ Internet Protocol Version 4, Src: 192.168.1.33 (192.168.1.33), D
⊞ Transmission Control Protocol, Src Port: xgrid (4111), Dst Port:
⊟ IEEE C37.118 Synchrophasor Protocol, Configuration Frame 2
  ⊞ Synchronization word: 0xaa31
    Framesize: 914
    PMU/DC ID number: 22
    SOC time stamp (UTC): 2013-03-19 23:20:59
  ⊞ Time quality flags
    Fraction of second (raw): 0
  ⊟ Configuration data, 1 PMU(s) included
      Resolution of fractional second time stamp: 16777215
      Number of PMU blocks included in the frame: 1
    ⊟ Station #1: "PHUNIT 1"
        PMU/DC ID number: 22
      ⊞ Data format in data frame
        Number of phasors: 11
        Number of analog values: 6
        Number of digital status words: 2
      ⊞ Phasor names (11)
      ⊞ Analog values (6)
      ⊞ Digital status labels (32)
```

OT Insurance

- It is now possible to buy cyber insurance for OT
- Expect:
  - Lengthy questionnaires
  - High cost (will come down as models improve)
  - Limits of 100Million in damages
  - Or 300 Million if you jump through every hoop
  - You may have audits or tests required
- READ EXCLUSIONS
  - Preferably with a legal advisor

Conclusions

It is far better to quantify and roleplay through a cyber disaster, then to have to manage one.

ROI is meaningless, you are risk reduction professionals.

Quantify a loss, learn many, many, lessons for your time and effort.

Centre for
Risk Studies

UNIVERSITY OF
CAMBRIDGE
Judge Business School