Cambridge Centre for Risk Studies

Risks and Benefits of Artificial Intelligence and Robotics – 6 February

The Cyber-Security Overlap

Centre for
Risk Studies

UNIVERSITY OF
CAMBRIDGE
Judge Business School

Session 3: the Cyber-Security Overlap Agenda

- The triangle of pain: the role of policy, public and private sectors in mitigating the cyber threat
  - Professor Daniel Ralph, Academic Director, Cambridge Centre for Risk Studies & Professor of Operations Research, University of Cambridge Judge Business School
- Modelling the cost of cyber catastrophes to the global economy
  - Simon Ruffle, Director of Research & Innovation, Cambridge Centre for Risk Studies
- Towards cyber insurance: approaches to data and modelling
  - Jennifer Copic, Research Associate, Cambridge Centre for Risk Studies

Cambridge Centre for Risk Studies

Risks and Benefits of Artificial Intelligence and Robotics – 6 February

The triangle of pain: the role of policy, public and private sectors in mitigating the cyber threat

Centre for **Risk Studies**

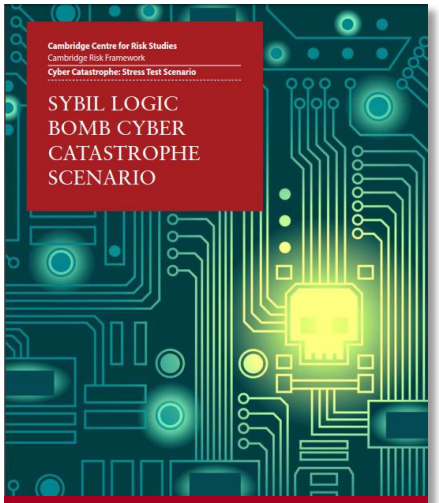
UNIVERSITY OF CAMBRIDGE
Judge Business School

Professor Daniel Ralph
Academic Director & Professor of Operations Research
Cambridge Centre for Risk Studies
& Cambridge Judge Business School

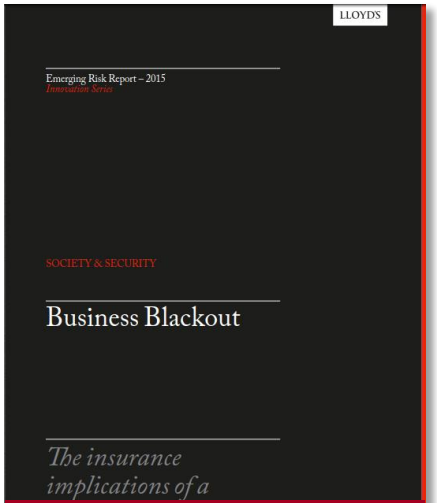
Centre for Risk Studies Mission Statement

To be the world's leading academic centre for research into systemic risk in business, the economy, and society

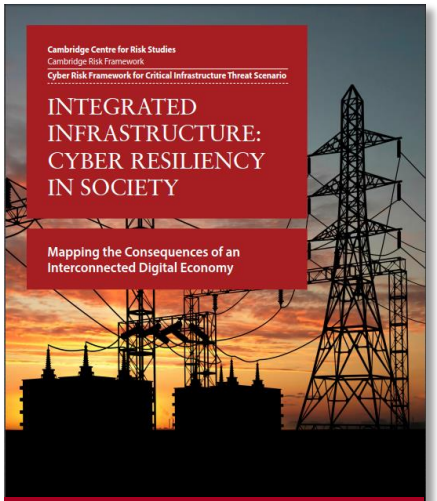
CCRS Cyber Research:
Stress Test Scenarios and Insurance Loss Models



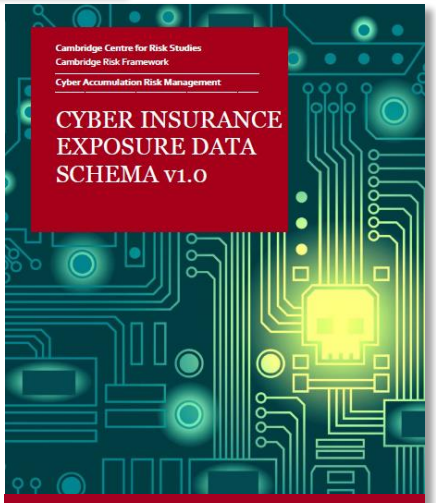
Sybil Logic Bomb



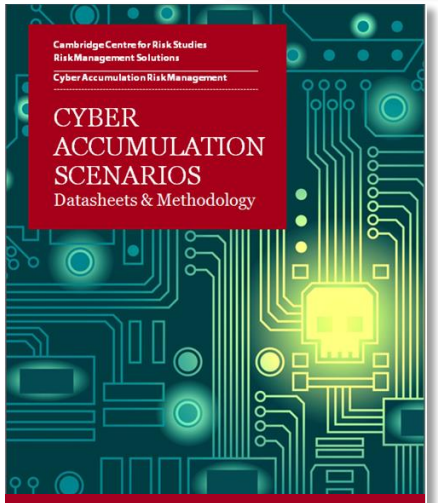
US Cyber Attack



UK Cyber Attack



Exposure Data Schema



Accumulation Scenarios

Cyber Terrorism

In preparation

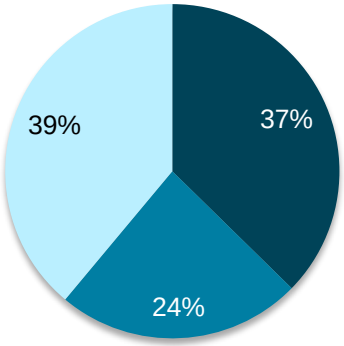
The Knowledge Economy

Old

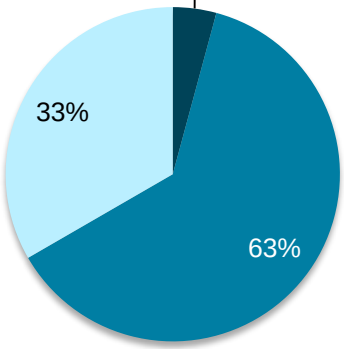
New

Economies categorised by dependency on critical infrastructure

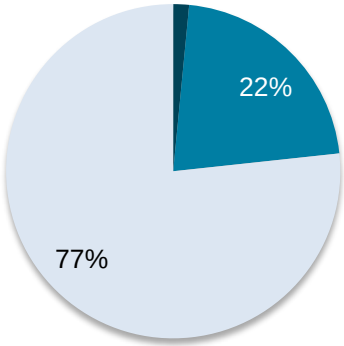
Agriculture with Industry & Service



Industrial-Oriented Economy



Service-Dominated Economy



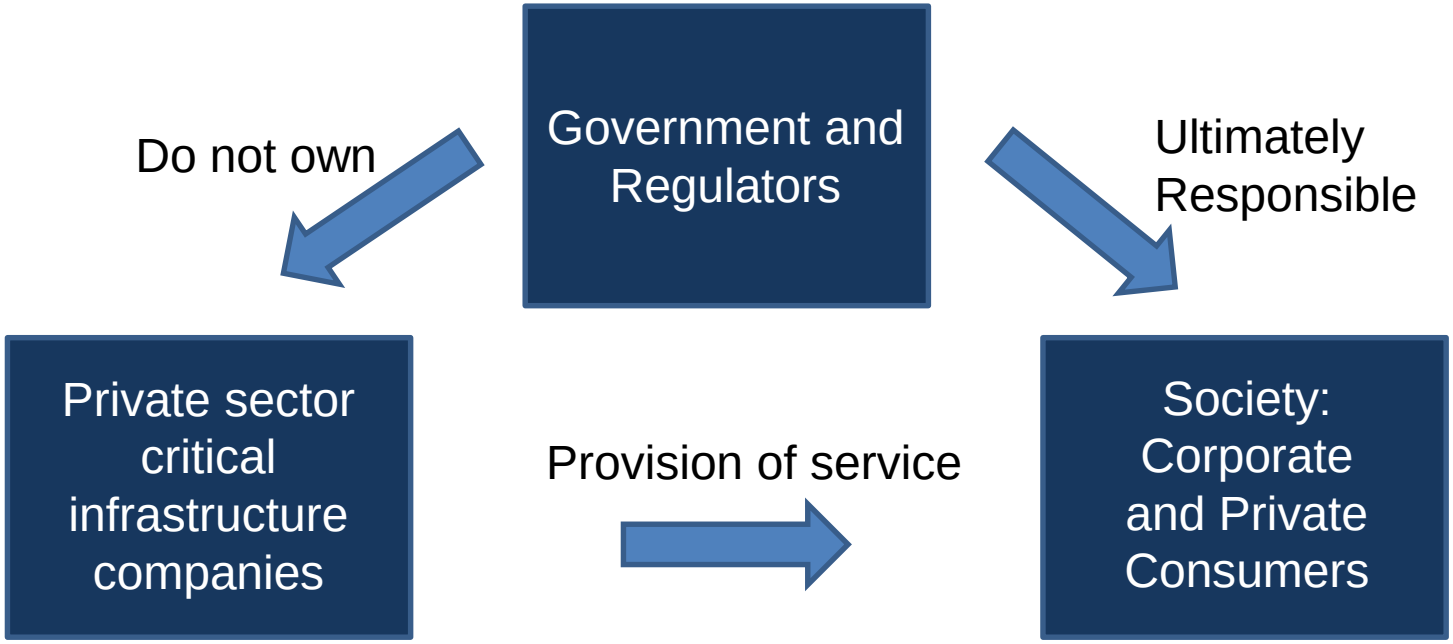
What is Cyber Risk?

- Cyber Risk
  - *"Any risk of financial loss, disruption or damage to the reputation of an organisation from some sort of failure of its information technology [or operational technology] systems"*

The Institute for Risk Management. "Cyber Risk". 2014

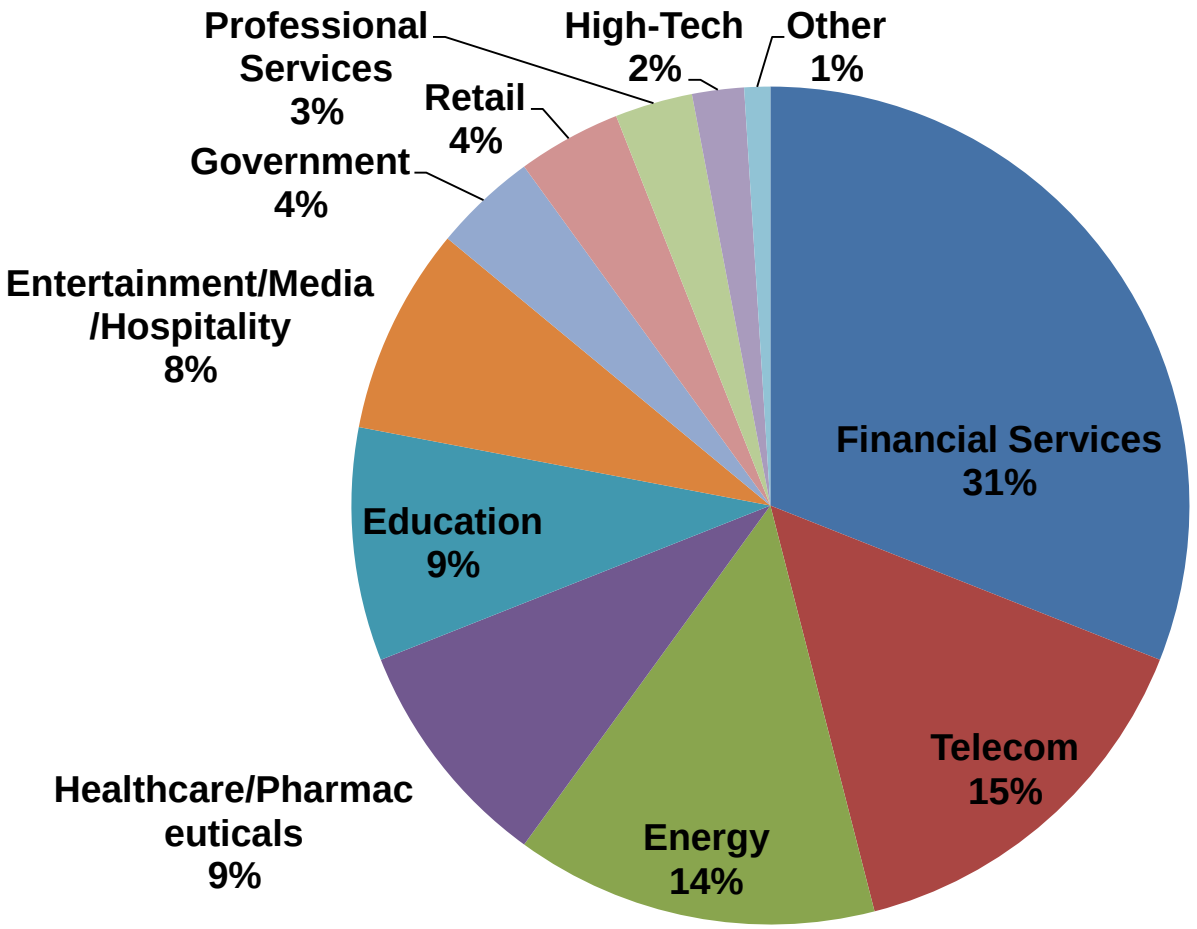
- IT (information technology)
  - Attacks on non-physical assets could target enterprise systems, such as websites or databases
- OT (operational technology)
  - Attacks on physical assets could target industrial control systems like SCADA and have the potential to cause physical damage

Triangle of Pain: Failure of Critical Infrastructure



Optimizing the risk equation: who bears the risk?

Cyber Attacks by UK Sector



Chandiramani, Yogi. "The FireEye Advanced Threat Report 2012: UK and Ireland Edition. 29 April, 2014. https://www.fireeye.com/blog/executive-perspective/2014/04/the-fireeye-advanced-threat-report-2013-uk-ireland-edition.html [Accessed: July 2015]

Historical UK Power Outages

- 1987

  Wind storm breaks the link between UK and France. SE East England w/out power for approximately 6 hours

- 2003

  Back to back transmission system faults caused a 34 minute power outage in parts of London. (London Assembly, 2004)

- 2009

  A power cut due to arson at a cable installation left 94,000 customers without power for four days (BBC, 2009)

- 2010

  A blackout in Portsmouth was caused by a substation fire, 47,000 people without power (BBC, 2010)

- 2013

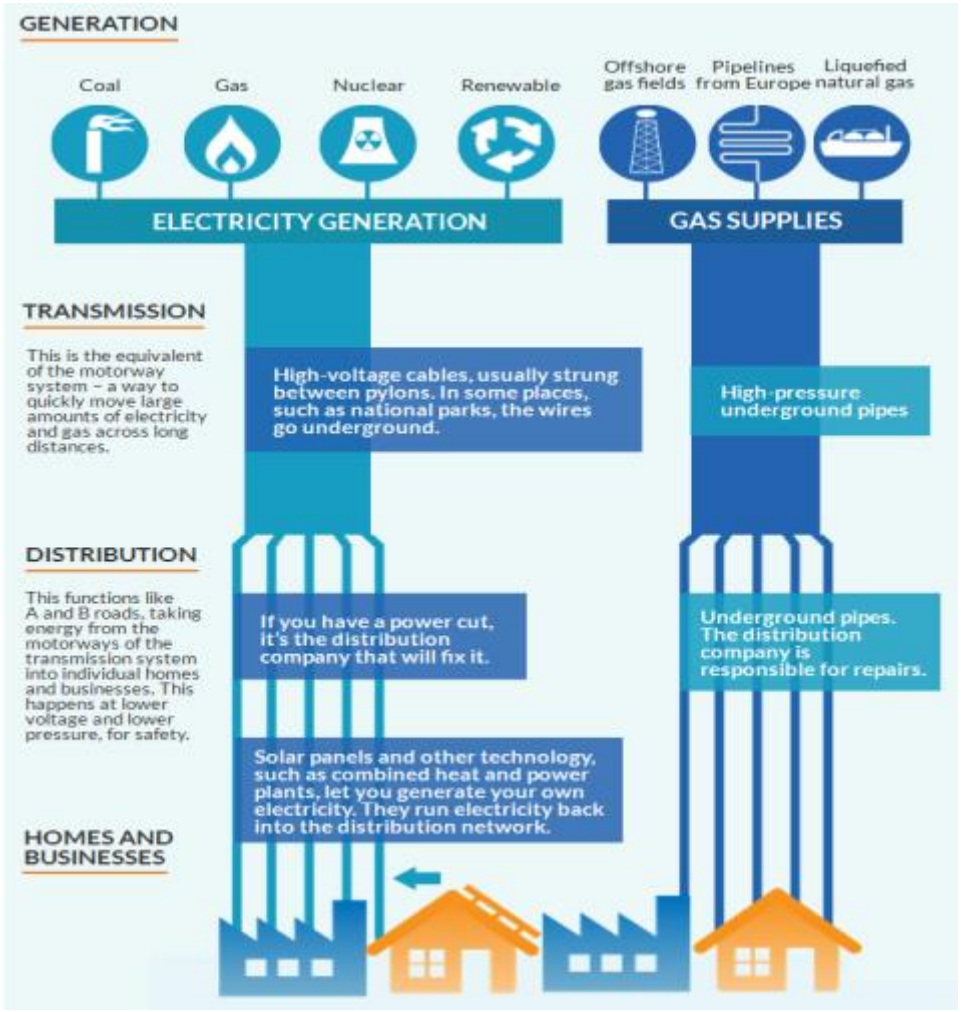
  Severe winter storms in Dec damaged distribution network affecting almost 1 million customers over 48 hours (Cabinet Office, 2015)

- 2015

  An underground fire in Holborn cable tunnels caused a power outage. It took 36 hours to put out the blaze (BBC, 2015)

London Wednesday 1 April 2015 [Picture: Twitter/@mdw1989]

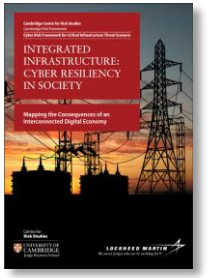
CRS Cyber Attack Scenarios on Power System



US Generation

EU Transmission
Future Project TBD

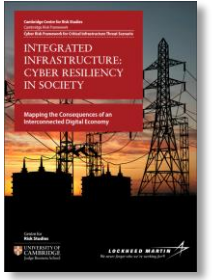
UK Distribution



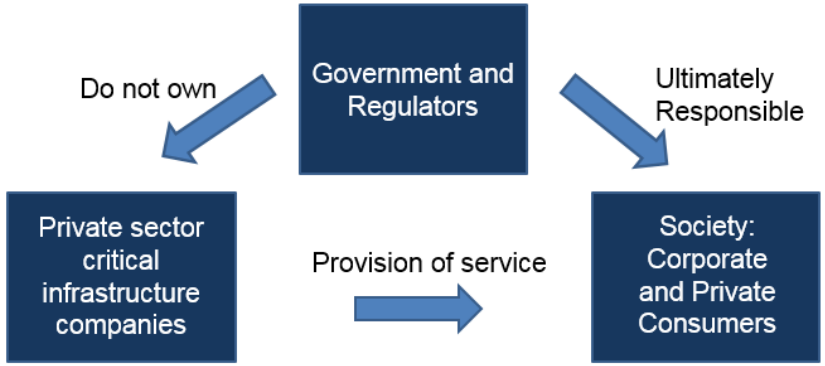
SmartGrid/Smart Cities
Future Project TBD

Source: https://www.ofgem.gov.uk/network-regulation-%E2%80%93-riio-model/energy-network-how-it-works-you

Electricity Distribution Under Threat From Cyber Attack

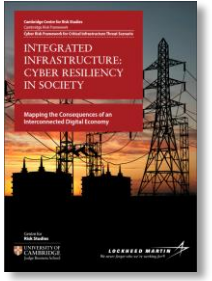


Triangle of Pain



Source: National Grid. “Distribution Network Operator (DNO) Companies”

2015 Ukraine Cyber Attack on Electricity Distribution Substations



- Power outage 23 December 2015
- Electricity outage affected region with over 200,000 people for several hours
- Malware (BlackEnergy) in 3 distribution substations
- Still investigating if switching came from hackers
  - The Ukrainian energy ministry probing a “suspected” cyber attack on the power grid
- Ukraine CERT confirms there was spear phishing at affected companies prior to outage

them.

FINANCIAL TIMES

D UK COMPANIES MARKETS OPINION WORK & CAREERS LIFE & ARTS

Cyber Security + Add to myFT

Hackers shut down Ukraine power grid

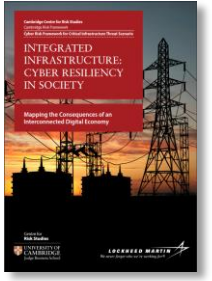
© AFP

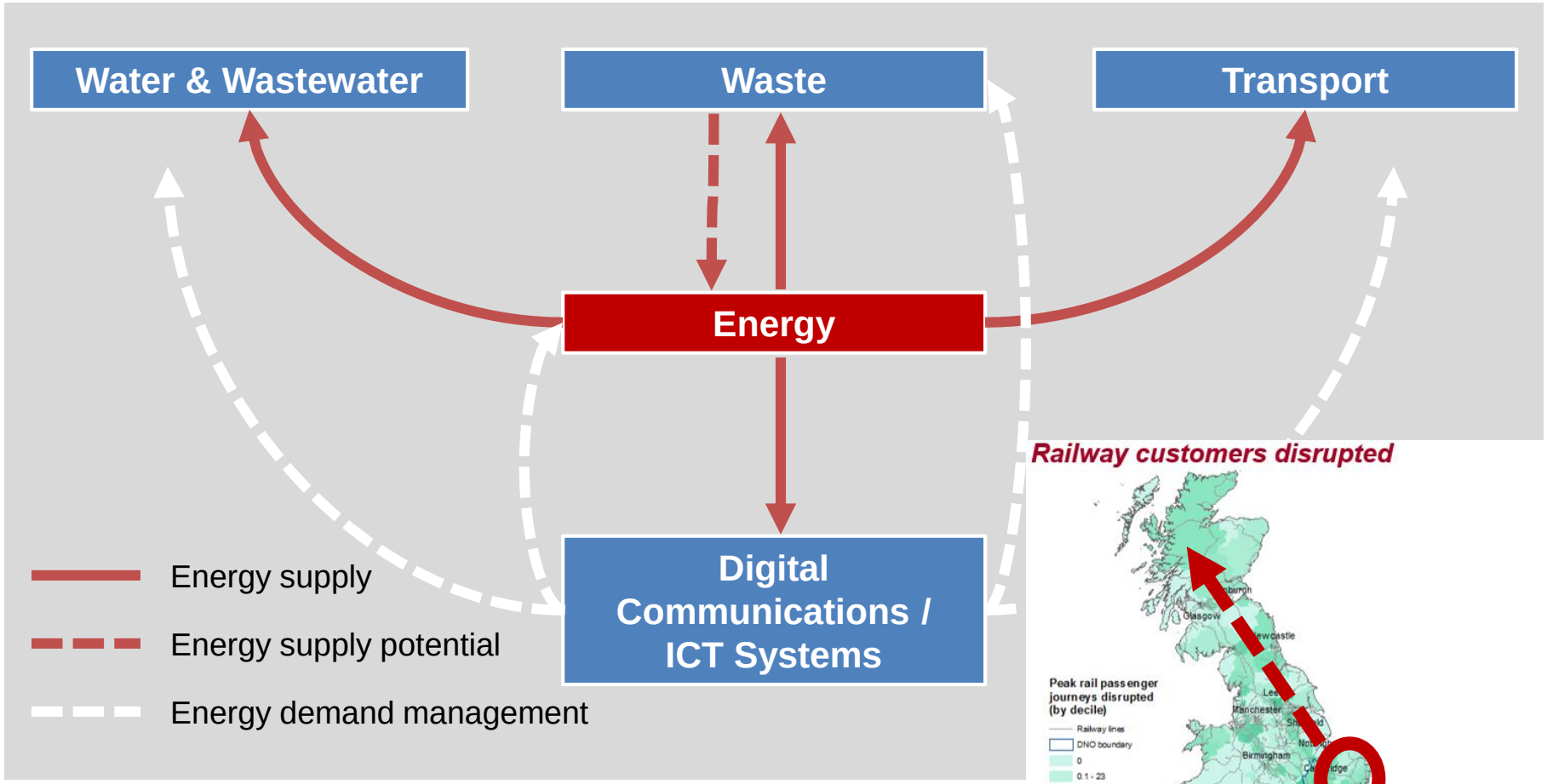
12 Save

JANUARY 5, 2016 by: Hannah Kuchler in San Francisco and Neil Buckley in London

Hackers brought down the power supply to hundreds of thousands of homes in Ukraine last week, in a cyber attack believed to be the first ever to result in a power outage.

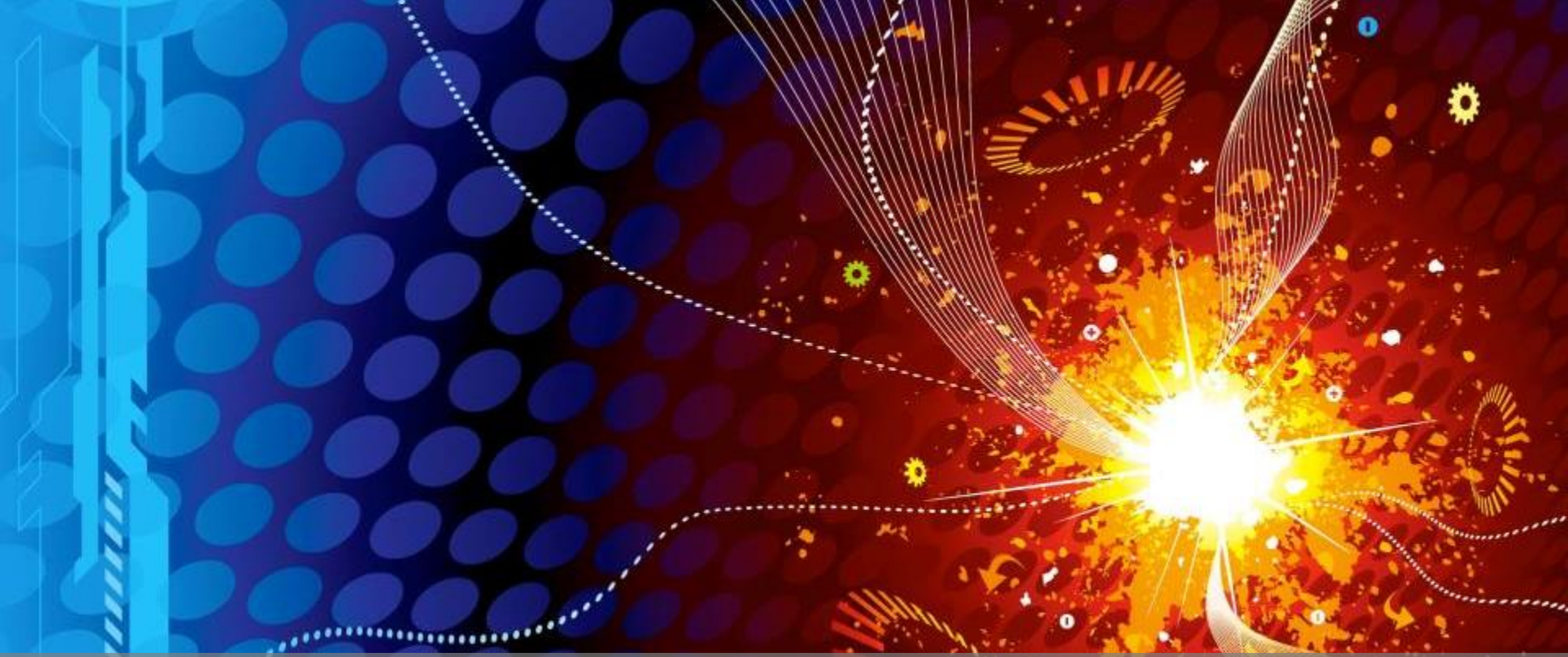
Growing Interdependency Amplifies the Triangle of Pain





Railway customers disrupted

Customer disruptions by scenario: S1 = 0.85m | S2 = 1m | X1 = 1m



Cambridge Centre for Risk Studies

Risks and Benefits of Artificial Intelligence and Robotics – 6 February

Modelling the cost of cyber catastrophes to the global economy

Centre for **Risk Studies**

UNIVERSITY OF CAMBRIDGE
Judge Business School

Simon Ruffle
Director of Research & Innovation
Cambridge Centre for Risk Studies

Catastrophe Modelling in Complex Systems

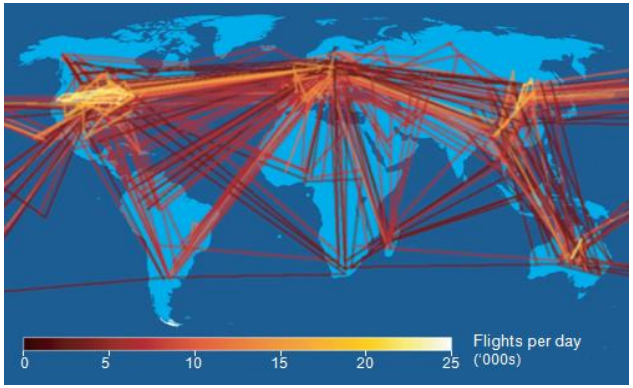
- The Centre for Risk Studies arises from shared interests by the participants in exploring areas of intersection between
  - Catastrophe modelling and extreme risk analytics
  - Complex systems and network failures
- Advance the scientific understanding of how systems can be made more resilient to the threat of catastrophic failures

To answer questions such as:

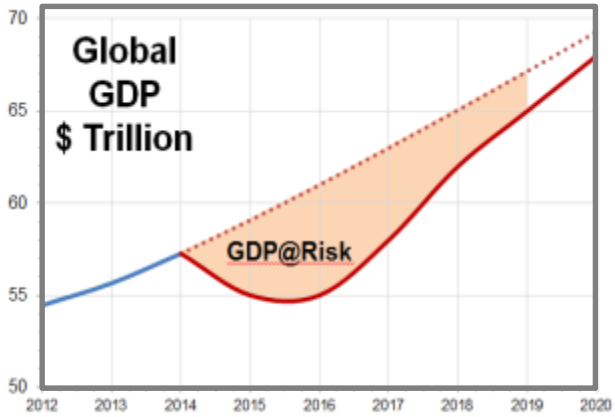
'What would be the impact of
a [War in China] on [Trade Networks] and how would this impact the [Global Economy]?

Regional Conflict

Air Travel Network



Global Economy



Cambridge Taxonomy of Threats

Financial Shock


Asset Bubble


Financial Irregularity


Market Crash


Sovereign Default

Bank Run

Trade Dispute

Labour Dispute


Trade Sanctions


Cartel Pressure


Nationalization


Tariff War

Geopolitical Conflict


Conventional War


Asymmetric War


External Force


Civil War


Nuclear War

Political Violence


Terrorism


Separatism


Organized Crime


Assassination


Social Unrest

Natural Catastrophe


Earthquake


Windstorm


Volcanic Eruption


Flood


Tsunami

Climatic Catastrophe


Drought


Freeze


Tornado & Hail


Electric Storm


Heatwave

Environmental Catastrophe


Sea Level Rise


Ocean System Change


Wildfire

Pollution Event

Atmospheric System Change

Technological Catastrophe

Nuclear Meltdown

Industrial Accident

Cyber Catastrophe

Technological Accident

Infrastructure Failure

Disease Outbreak

Human Epidemic

Animal Epidemic

Waterborne Epidemic

Zoonosis

Plant Epidemic

Humanitarian Crisis

Famine

Water Supply Failure

Child Poverty

Welfare System Failure

Refugee Crisis

Externality

Meteorite

Solar Storm

Space Threat

Ozone Layer Collapse

Satellite System Failure

Other

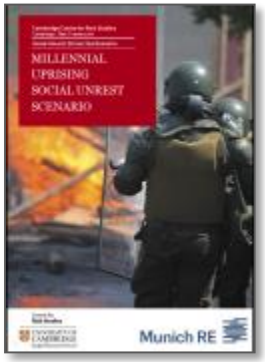
CCRS Research Outputs: Explorations of individual threats

Taxonomy of Threats

Geopolitical Conflict
Emerging Risk Scenario

Pandemic
Emerging Risk Scenario

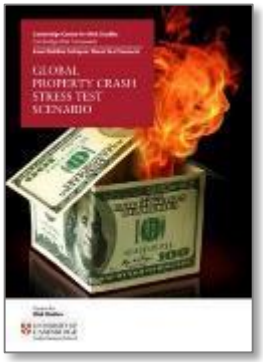
Cyber Catastrophe
Emerging Risk Scenario



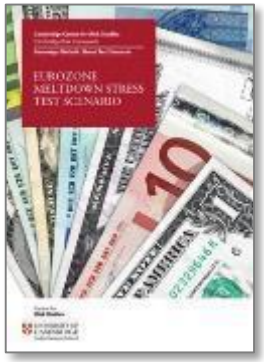
Social Unrest
Emerging Risk Scenario

Ebola
Emerging Risk Scenario

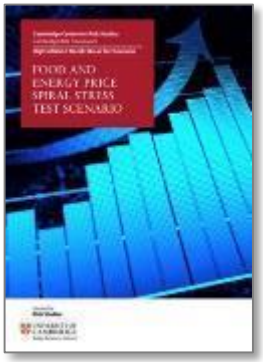
Financial Catastrophes



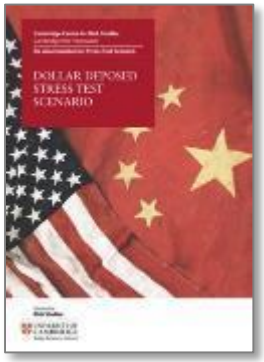
Global Property Crash
Financial Risk Scenario



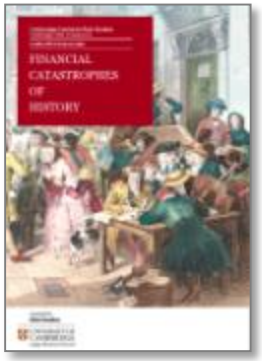
Eurozone Meltdown
Financial Risk Scenario



High Inflation
Financial Risk Scenario



Dollar Dethroned
Financial Risk Scenario

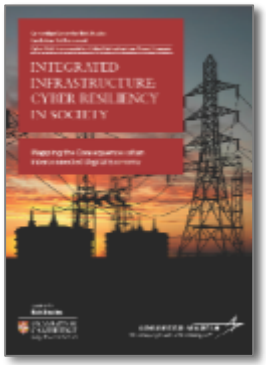


Historical Crises
Financial Risk

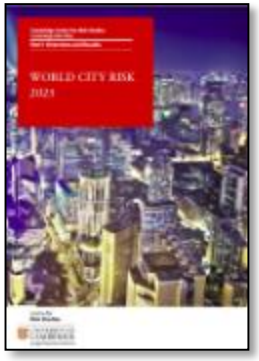
Cyber Accumulation
Insurance Risk Report

NatCat FinCats
Clash Report

Business Blackout
Lloyds Emerging Risk Report



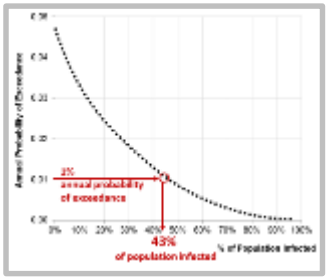
Infrastructure
Cyber Attack UK



World City Risk 2025
Lloyds Co-Branded Report

Solar Storm
Emerging Risk Scenario

Scenario Development Process



Historical Context

A justification and context for a 1% annual probability of occurrence worldwide

Timeline & Footprint

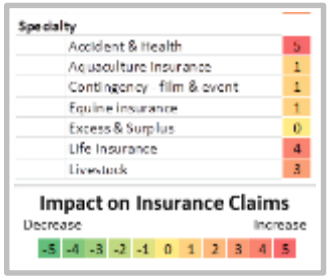
Sequencing of events in time and space in hypothetical scenario

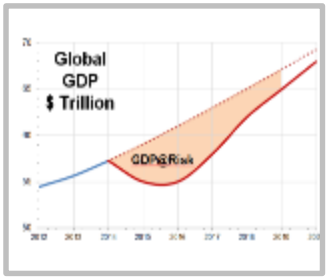
Narrative

Detailed description of events
3-4 variants of key assumptions for sensitivity testing

Loss Assessment

Metrics of underwriting loss across many different lines of insurance business



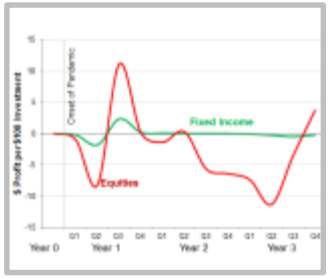


Macroeconomic Consequences

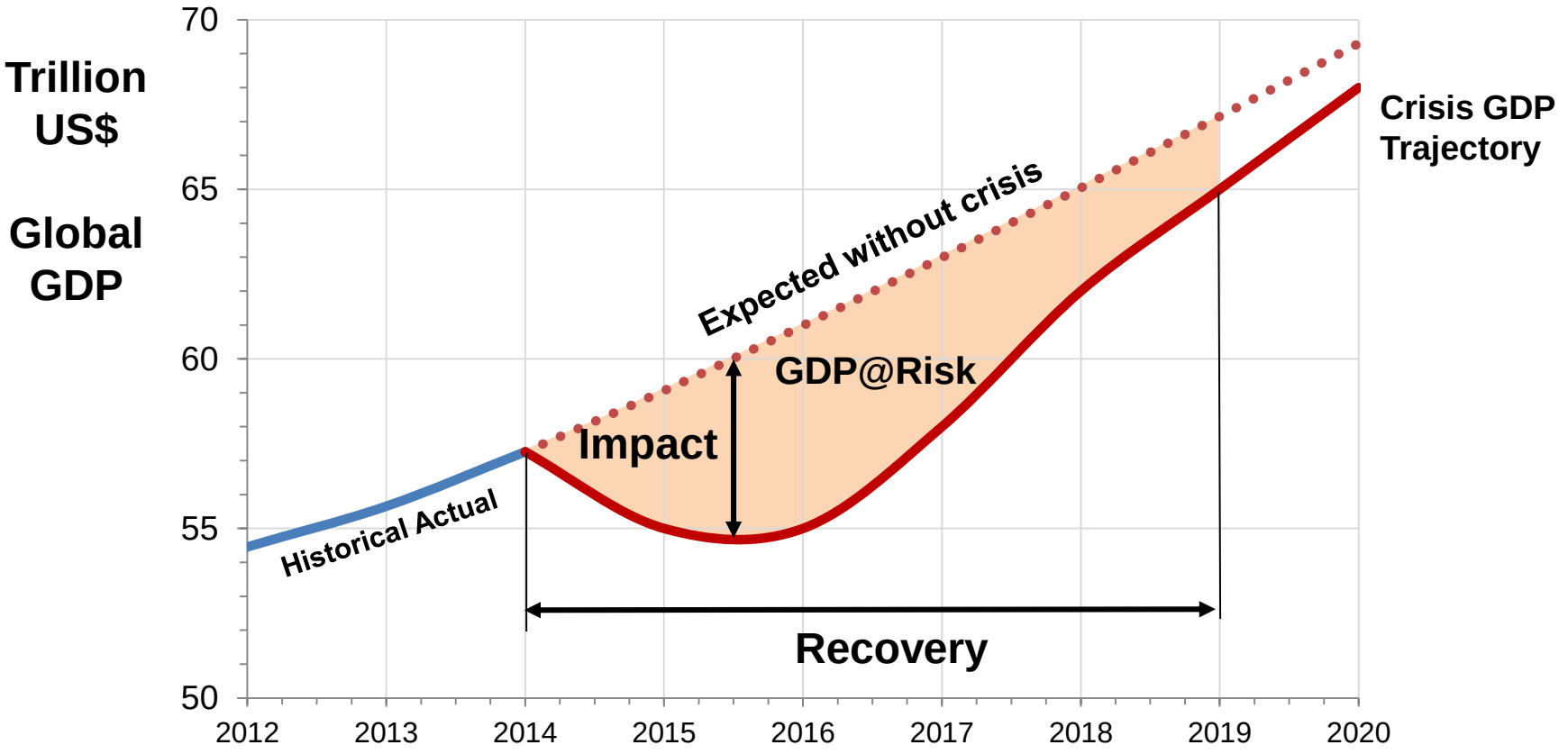
Quantification of effects on many variables in the global economy

Investment Portfolio Impact

Returns and performance over time of a range of investment assets



Catastronomics: GDP@Risk



GDP@Risk: Cumulative first five year loss of global GDP, relative to expected, resulting from a catastrophe or crisis

Cyber Risk Research at CCRS

IT Scenarios
Information Technology

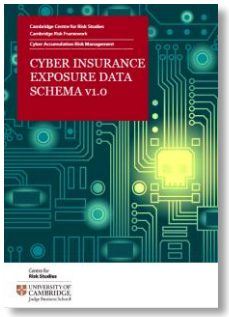
- **Data Exfiltration** ('Leakomania')
- **Denial of Service Attack** ('Mass DDoS')
- **Cloud Service Provider Failure** ('Cloud Compromise')
- **Financial Theft** ('Cyber Heist')
- **Ransomware** ('Extortion Spree')
- **Malware** ('Sybil Logic Bomb")

OT Scenarios
Operations Technology

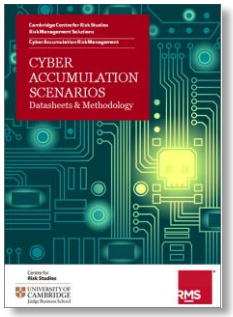
- Cyber Attack on **US Power Generation** ('Business Blackout')
- Cyber Attack on **UK Power Distribution** ('Integrated Infrastructure')
- Cyber attack on **Commercial Office Buildings** (Laptop batteries fire induction')
- Cyber attack on **Marine Cargo Port** ('Port Management System')
- Cyber Attack on **Industrial Chemical Plant** ('ICS Attack')
- Cyber Attack on **Oil Rigs** ('Phishing-Triggered Explosions')

Sybil Logic Bomb

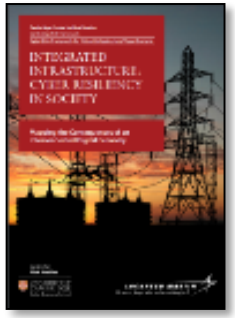
US Cyber Blackout



Exposure Data Schema



Accumulation Scenarios



UK Cyber Blackout

Cyber Terrorism

Malware: the ‘Erebos’ Trojan

- Erebos is the Greek God of Darkness
- Understand the scale of loss
  - We have not yet had ‘the Big One’ for cyber
  - This fictional event explores what a cyber catastrophe might look like
- Insurance industry needs to quantify the size of the loss
- Malware trojans
  - A team of software hackers creates the ‘Erebos’ Remote Access Trojan
  - The Erebos Trojan is a fictional piece of malware that can infect generator control rooms that goes undetected
  - When activated it finds generators with specific characteristics and forces them to burn out

The Aurora Vulnerability:
Phase Angle De-Synchronisation of a Generator

US Electricity Grid Interconnections

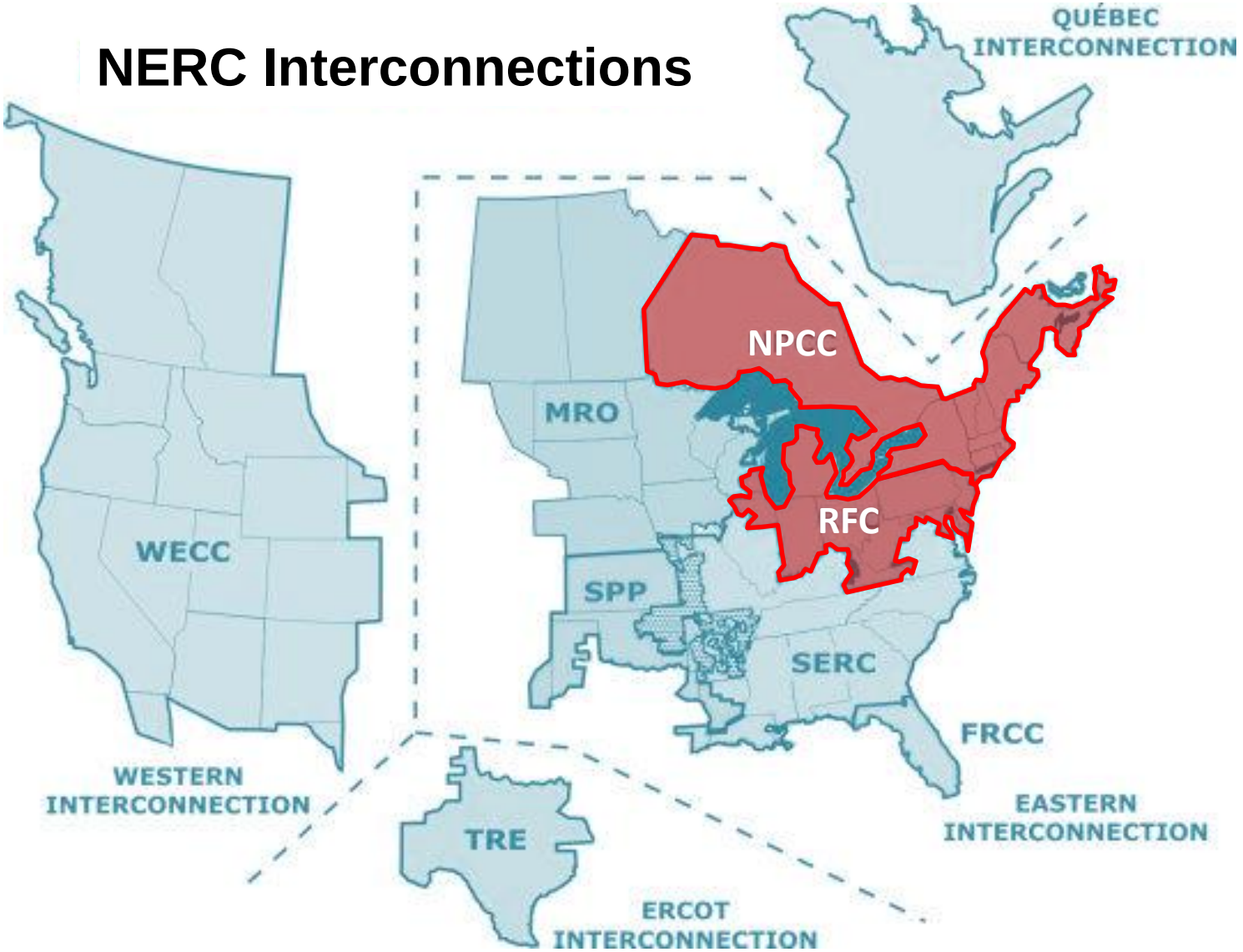
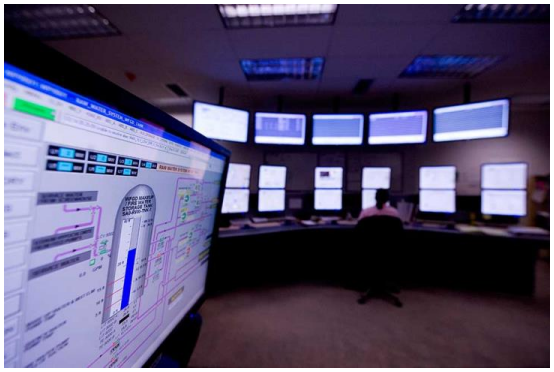


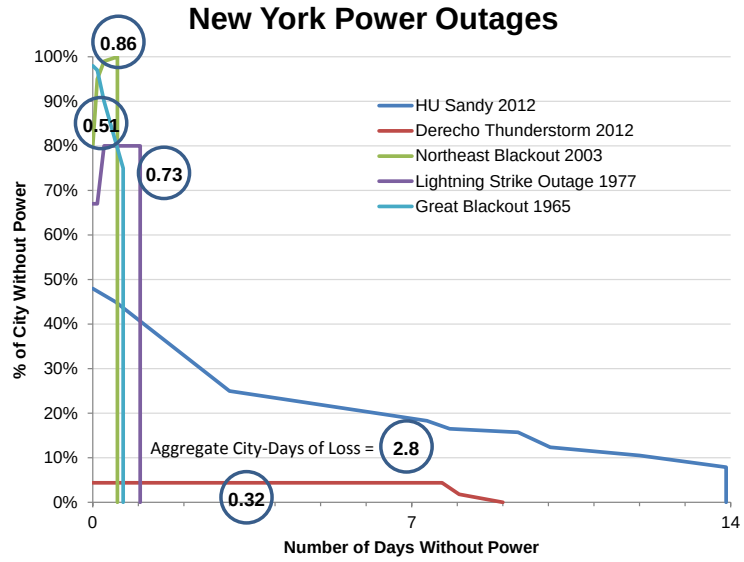
Image Source: North American Electric Reliability Corporation; 2013, *Regional Entities, NERC Interconnections* [Online] Available: http://www.nerc.com/AboutNERC/keyplayers/Pages/Regional-Entities.aspx/

Erebos Business Blackout Scenario

- During peak summer demand for electricity – there is a coordinated simultaneous attack targeted at two regions of United States power grid (NPCC and RFC)
- Malware finds 50 generators that it can control and forces them to overload and burn out
  - in some cases causing additional fires and explosions
- Electricity blackout that plunges 15 US states and Washington DC into darkness
- 93 million people without power
- More than 17 TW-Hours of generation is lost – around 12% of supply

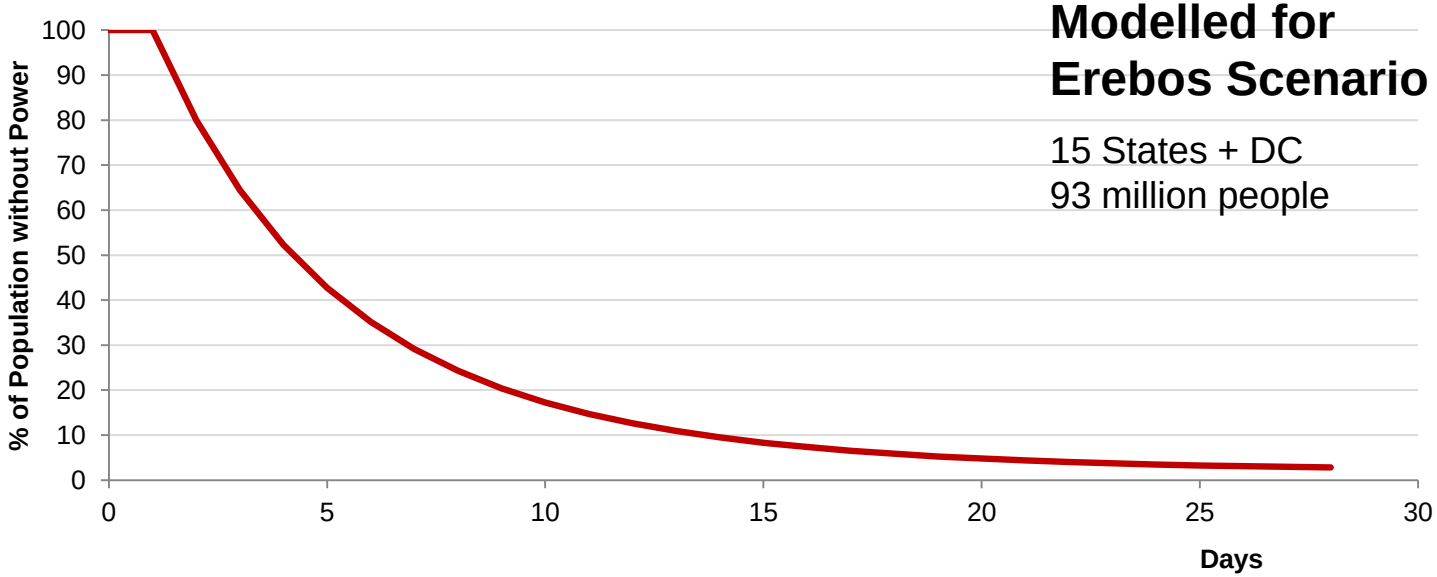


Outage & Restoration of Power



Historical Examples

New York
8 million people

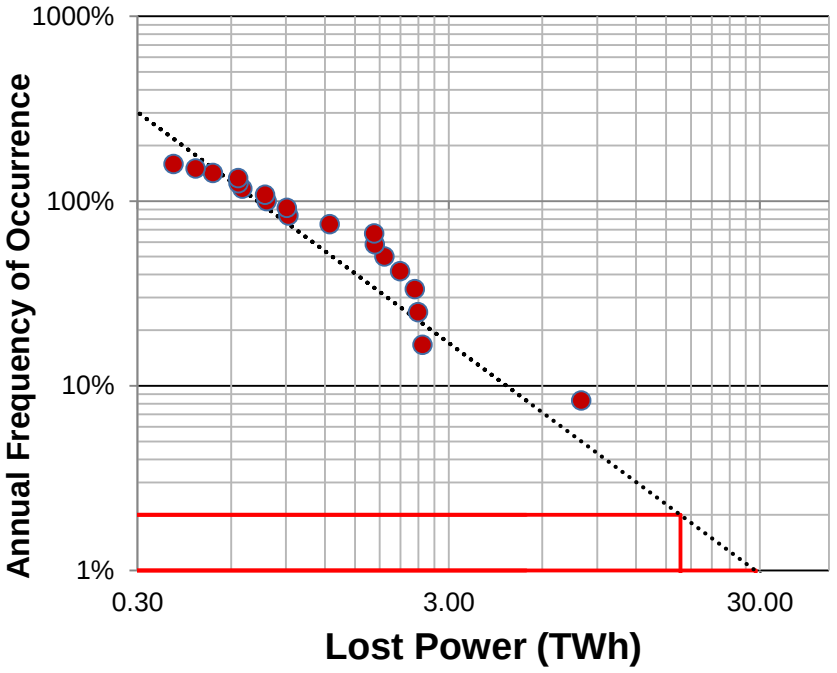


Modelled for Erebos Scenario

15 States + DC
93 million people

Scenario Outage Levels Comparable with Extreme Weather

- Generation supply loss in our scenario is equivalent to extreme outage levels expected from US **weather events**
- Historical data suggests a weather-related outage of around 17 TW-hours can be expected with an annual probability of 2%
- We are not assigning a probability to a cyber attack
  - The return period of our scenario is unknown
  - We are providing historical weather disruption for context

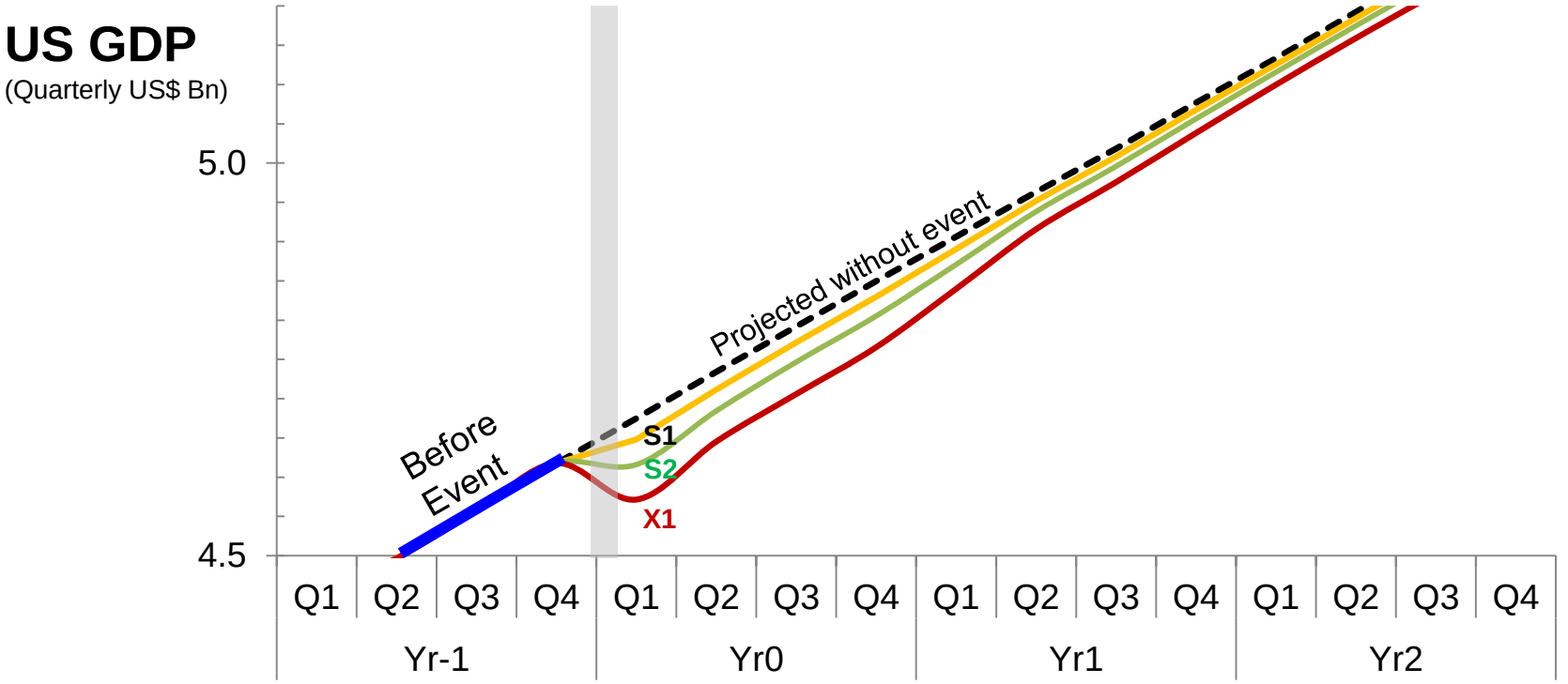


Scenario variants

Peak Demand	**190 GW**
Demand Over 30 days	**136.8 TWh**

S1	S2	X1
13%	27%	46%
17 TWh	**37** TWh	**63** TWh

Economic Impact: GDP@Risk



Scenario Variant	Outage Duration (to 90% reconnected)	Consumption	Labour	Exports	Confidence	GDP@Risk (5 Yr)
S1	2 Weeks	0.6%	0.6%	1.3%	5%	**$243 Bn**
S2	3 Weeks	1.3%	1.3%	2.8%	10%	**$544 Bn**
X1	4 Weeks	2.2%	2.2%	4.9%	20%	**$1,024 Bn**

Shocks are a proportion of total US output over 1Q

Summary of Erebos Business Blackout Scenario

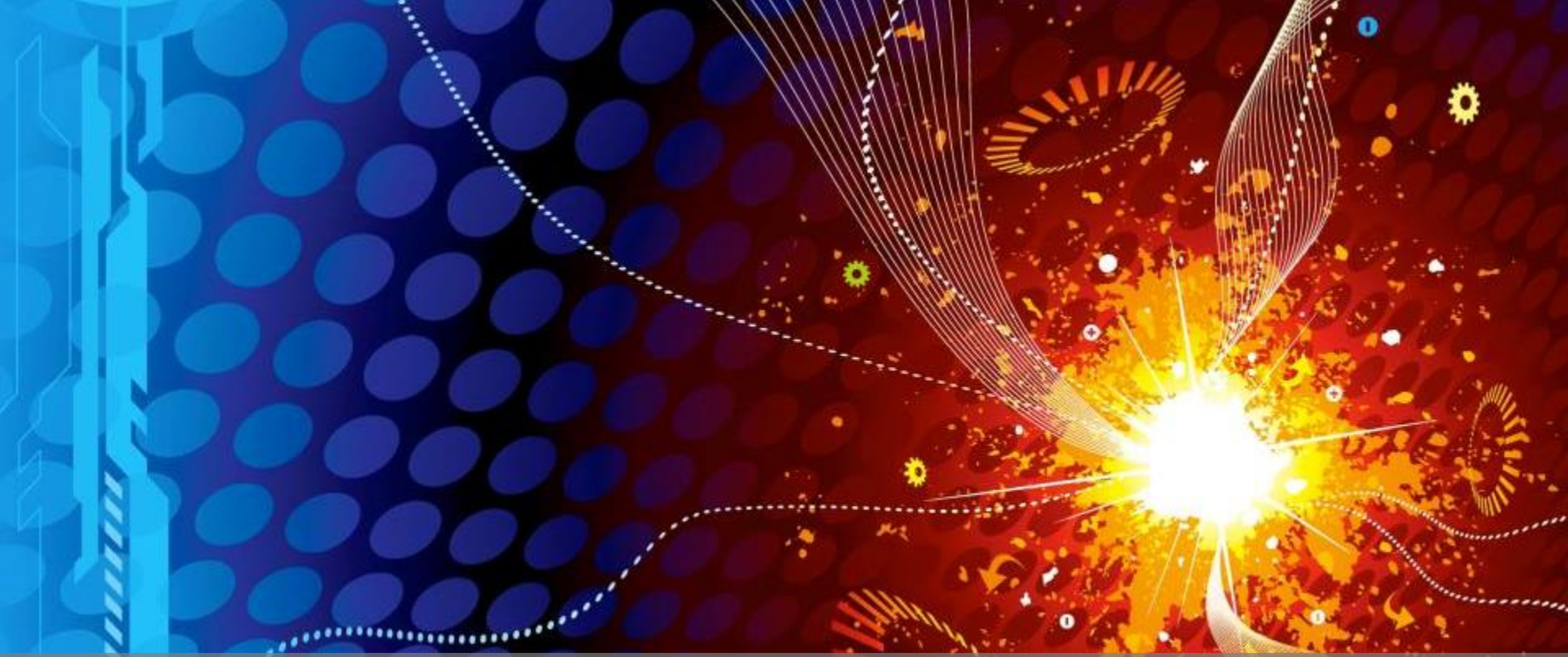
Scenario Variant	Outage Duration (to 90% reconnected)	Number of Generators Damaged	Economic Output Lost GDP@Risk	Insurance Industry Loss Estimate
S1	2 Weeks	50	$243 Bn	$21.4 Bn
S2	3 Weeks	50	$544 Bn	$39.9 Bn
X1	4 Weeks	100	$1,024 Bn	$71.1 Bn

For context:

- Total insurance catastrophe losses 2014: $45 Bn
- Hurricane Katrina 2005: $80 Bn
- Tohoku Earthquake Japan 2011: $38 Bn
- Superstorm Sandy 2012: $37 Bn
- Hurricane Andrew 1992: $28 Bn
- 9/11 WTC 2001: $26 Bn

[2015 $ value]

Full details of insurance loss estimation methodology :
http://www.lloyds.com/news-and-insight/risk-insight/library/society-and-security/business-blackout



Cambridge Centre for Risk Studies

Risks and Benefits of Artificial Intelligence and Robotics – 6 February

Towards cyber insurance: approaches to data and modelling

Centre for **Risk Studies**

UNIVERSITY OF CAMBRIDGE
Judge Business School

Jennifer Copic
Research Associate
Cambridge Centre for Risk Studies

Insurance and Cyber Risk

- Insurance is a risk transfer tool for corporates trying to manage this emerging risk
- Cyber offers potential for market growth and new product development
- Insurers are concerned with accumulation risk due to the potentially systemic impact of an event
  - Regulators are also concerned of accumulation risk in the market
- Insurers themselves have operational exposure to cyber risk

Four Different Types of Cyber Insurance Exposure

1. **Affirmative Standalone Cyber Cover**: Specific standalone policies for data breach, liabilities, property damage and other losses resulting from information technology failures, either accidental or malicious
   - This is generally known as cyber liability insurance cover (CLIC)
   - Technology errors and omissions (E&O) liability insurance, available as a specific insurance product for the providers of technology services or products to cover both liability and other loss exposures.
2. **Affirmative Cyber Endorsements**: Cyber endorsements that extend the coverage of a traditional insurance product, such as commercial general liability
3. **Silent Cyber Exposure – Gaps in Explicit Cyber Exclusions**: There are a range of traditional policies, such as commercial property insurance, that have exclusion clauses for malicious cyber attacks
   - Except certain nominated perils such as: Fire; Lightning; Explosion and Aircraft Impact (FLEXA)
4. **Silent Cyber Exposure – Policies without Cyber Exclusions**: Many insurance lines of business incorporate ‘All Risks’ policies without explicit exclusions or endorsements for losses that might occur via cyber attacks

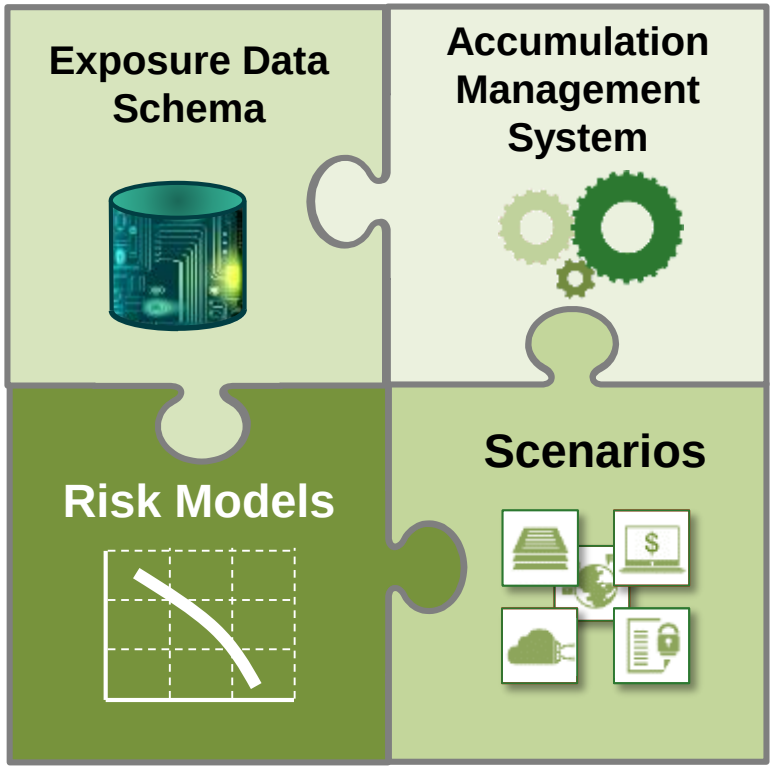
Cyber Loss Coverage Categories

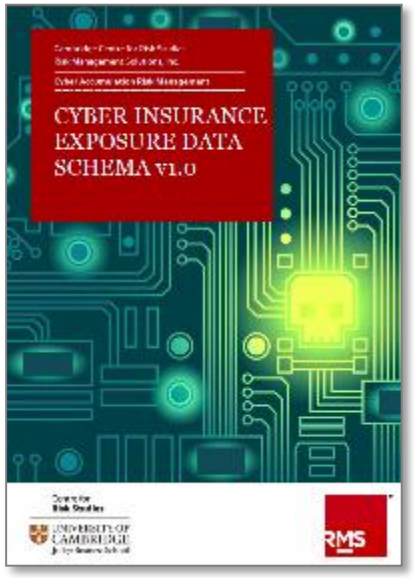
- Wide variation in coverage language
  - No two cyber products are the same
- Additionally, insurers need to capture cyber attribute data, such as
  - Number of records of PII
  - Named cloud providers
  - Named payment system providers

v1.0 Code	Cyber Loss Coverage Category	% of Products Offering this Cover (Sample of 26)
1	Breach of privacy event	92%
2	Data and software loss	81%
6	Incident response costs	81%
15	Cyber extortion	73%
4	Business interruption	69%
12	Multi-media liabilities (defamation and disparagement)	65%
7	Regulatory and defence coverage	62%
14	Reputational damage	46%
3	Network service failure liabilities	42%
5	Contingent Business Interruption	33%
9	Liability – Technology Errors & Omissions	27%
10	Liability – Professional Services Errors & Omissions	23%
13	Financial theft & fraud	23%
16	Intellectual property (IP) theft	23%
18	Physical asset damage	19%
19	Death and bodily injury	15%
11	Liability – Directors & Officers	13%
8	Liability – Product and Operations	8%
17	Environmental damage	4%

Coverage categories adapted from UK Government and Marsh, UK Cyber Security: The Role of Insurance in Managing and Mitigating the Risk, March 2015

Cyber Catastrophe Scenarios for Insurance Accumulation Management





Jan 2016
v1.0
First complete schema

Industry Organizations Supporting the Schema

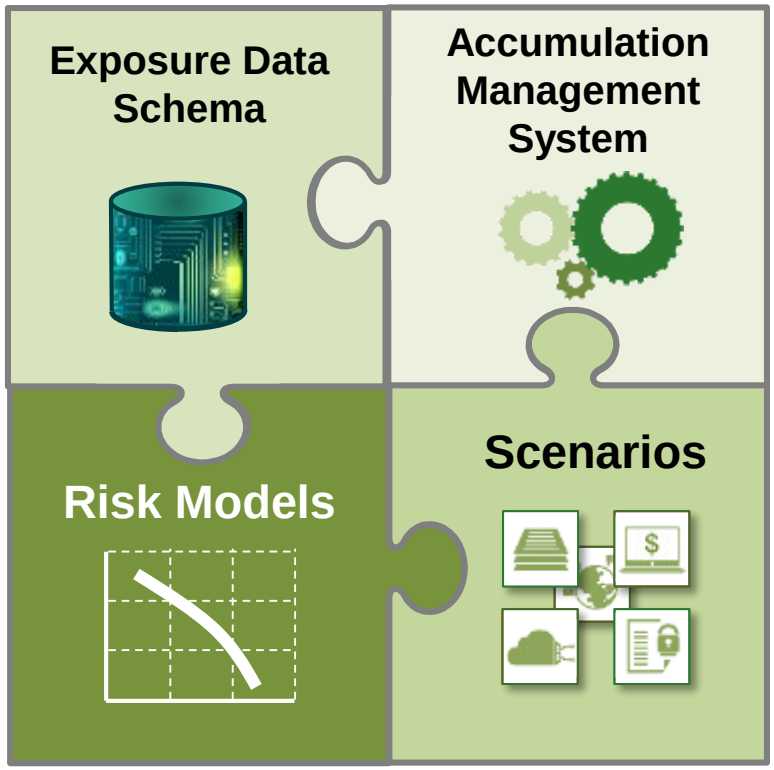
Reinsurance Association of America

Lloyd's

Lloyd's Market Association

Chief Risk Officer Forum

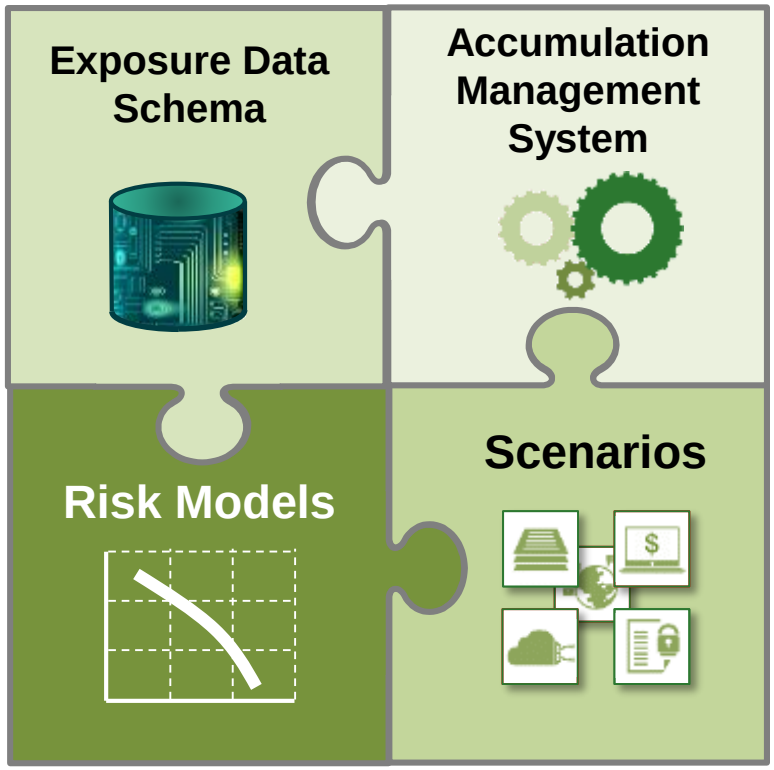
Cyber Catastrophe Scenarios for Insurance Accumulation Management



Affirmative cyber attack scenarios developed by Centre for Risk Studies
Deployed in CAMS v1.0

- **Data Exfiltration** ('Leakomania')
- **Denial of Service Attack** ('Mass DDoS')
- **Cloud Service Provider Failure** ('Cloud Compromise')
- **Cyber Heist** ('Financial Theft')
- **Ransomware** ('Extortion Spree')
- **ShadowBrokers** ('ExtraBacon Exploited')

Cyber Catastrophe Scenarios for Insurance Accumulation Management



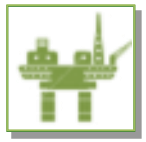
UNIVERSITY OF CAMBRIDGE Judge Business School | Centre for Risk Studies

Silent cyber attack scenarios developed by Centre for Risk Studies
Deployed in CAMS v2.0

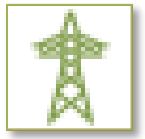
Cyber-Induced Fires in Commercial Office Buildings (Laptop batteries fire induction')

Cyber-Enabled Marine Cargo Theft from Port ('Port Management System')

ICS-Triggered Fires in Industrial Processing Plants ('ICS Attack')



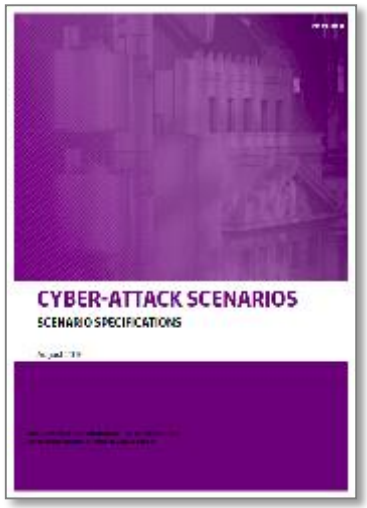
PCS-Triggered Explosions on Oil Rigs ('Phishing-Triggered Explosions')



Regional Power Outage from Cyber Attack on US Power Generation ('Business Blackout') S1, X1

Regional Power Outage from Cyber Attack on UK Power Distribution ('Integrated Infrastructure')

Lloyd's Cyber Realistic Disaster Scenarios (RDS)



	CRS Cyber Scenarios
1. Data Theft from an Aggregator	**Data Exfiltration** (Variant of 'Leakomania')
2. Cloud Computing Service Provider	**Cloud Service Provider Failure** ('Cloud Compromise' Reference View)
3. Northeast Blackout Scenario S1	Attack on **US Power Generation** ('Business Blackout Scenario S1')
4. Northeast Blackout Scenario X1	Attack on **US Power Generation** ('Business Blackout Scenario X1')
5. UK Blackout Scenario	Attack on **UK Power Distribution** ('Integrated Infrastructure')
6. Offshore Energy – MODU DP attack	Version in development Different attack vector
7. Aviation – navigation control attack	
8. Marine – ballast control system attack	Version in development Different attack vector

Lloyd's have opted to only require the Northeast Blackout (Erebos) Scenario for future reporting

Insurance Loss Estimate

Power Generation Companies		$ millions
	Property Damage (Generators)	633
	Business Interruption (Generator Damage)	3,817
	Incident Response Costs	3
	Fines - FERC/NERC	4
	Other liabilities	-
Defendant Companies		
	Liability	2,253
Companies that Lose Power		
	Perishable Contents	595
	Contingent Business Interruption - Suppliers Extension	6,769
	Liability	3,120
Companies Indirectly Affected		
	Contingent Business Interruption - Critical Vendor	2,928
	Liability	749
Homeowners		
	Household Contents	465
Specialty		
	Event Cancellation	63
Total		**$ 21,398**

For variant S1

Panel Discussion 1: Triangle of Pain

- Accountability and responsibility of cyber
- When there is a disassociation of asset owners to customers and markets, who has culpability?
- Are there sector views?
  - Health
  - Energy
  - Media

Panel Discussion 2: Economic Consequences of Cyber

Total GDP loss is on scale of some large natural catastrophe events

- Would the public find GDP loss compelling within the cyber security discussion?
- What other metrics might the public find more informational than GDP loss?
- What are some other consequences of a large scale cyber threat?

Panel Discussion 3: Regulation of Cyber

Regulation exists to address health, safety, standards, public good, etc.

- Currently, lack of governmental incentives in regulation on cyber security standards for preparedness.
- What might a regulator of cyber look like for different sectors; major considerations?
  - Health
  - Energy
  - Media

Panel Discussion 4: Final Thoughts on Cyber

- Is there a step change in the way cyber security threats should be considered in the future?
- How can cyber security threats be managed as AI & autonomous systems become more pervasive
  - Health
  - Energy
  - Media

Centre for
Risk Studies

UNIVERSITY OF
CAMBRIDGE
Judge Business School

http://www.jbs.cam.ac.uk/faculty-research/centres/risk/