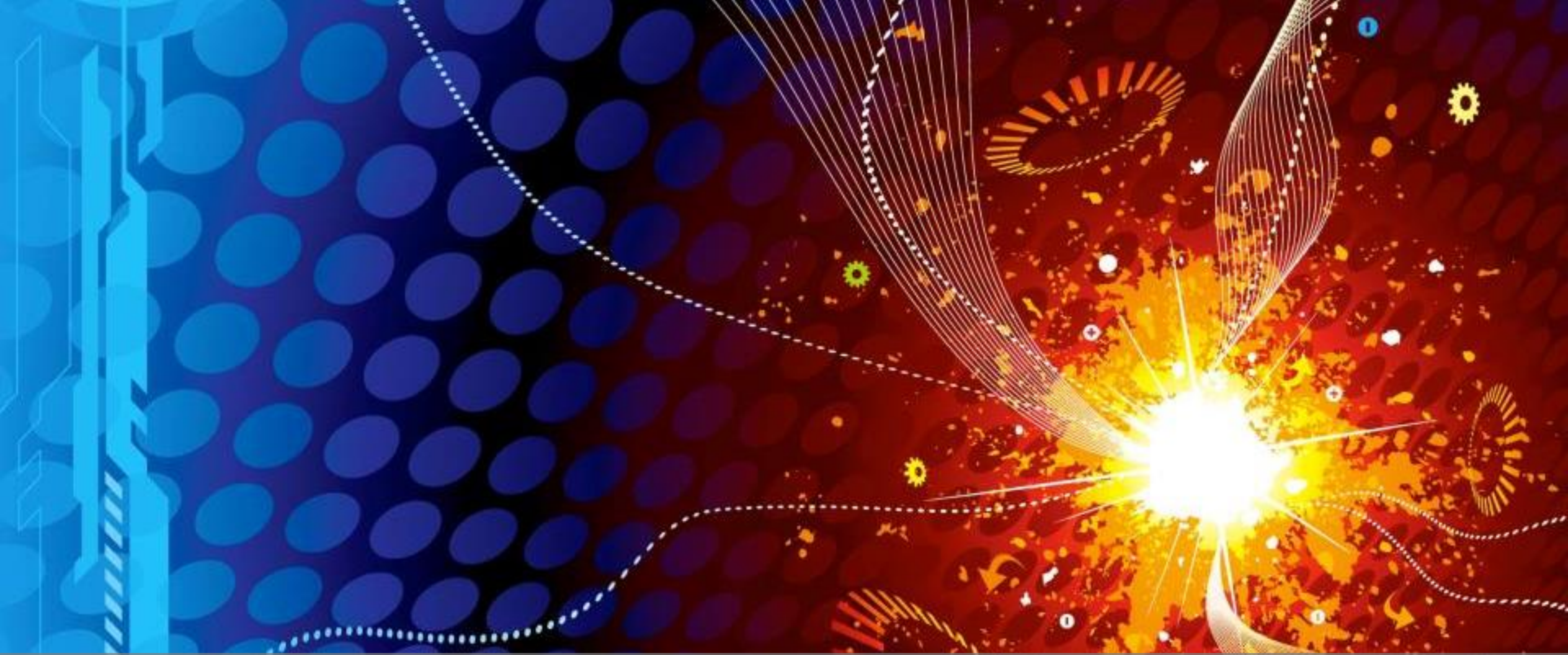


Cambridge Centre for Risk Studies

Advisory Board Research Showcase – 24 January 2017

Cyber Risk Research at CCRS

Centre for
Risk Studies

UNIVERSITY OF
CAMBRIDGE
Judge Business School

Jennifer Copic
Research Assistant
Cambridge Centre for Risk Studies

Largest Cyber Data Exfiltration Event: Yahoo

- August 2013 – 1 billion customer details such as phone numbers, birthdates, and security questions
  - Shares lost 6.5% after the announcement of this breach in Dec 2016
  - Hackers forged cookies in order to steal the information
- Late 2014 - 500 million records stolen in separate event announced in Sept 2016
- July 2016 – Verizon announced to buy Yahoo for $4.8 billion prior to the hacks being discovered
  - Verizon is exploring price cut due to the data breaches
  - Impact of Yahoo Data Breach could potentially kill the valuation of Yahoo

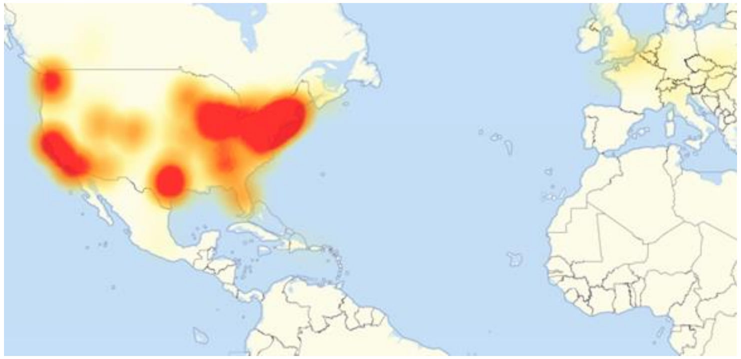
Leswing, K. "Yahoo confirms major breach — and it could be the largest hack of all time". Business Insider. 22 Sept 2016. http://uk.businessinsider.com/yahoo-hack-by-state-sponsored-actor-biggest-of-all-time-2016-9?r=US&IR=T

Weinberger, M. "IT HAPPENED AGAIN: Yahoo says 1 billion user accounts stolen in what could be biggest hack ever" Business Insider. 14 Dec 2016. http://uk.businessinsider.com/yahoo-data-breach-billion-accounts-2016-12

Moritz, S. and Womack, B. "Verizon Explores Lower Price or Even Exit From Yahoo Deal". Bloomberg Technology. 15 Dec 2016. https://www.bloomberg.com/news/articles/2016-12-15/verizon-said-to-explore-lower-price-or-even-exit-from-yahoo-deal

DDoS Attack on Dyn

- Dyn is an internet traffic management product managing domain name system (DNS) infrastructure
  - They promise to protect companies from DDoS
- They suffered two 2 hours outages due to a DDos attack as large as 1,200 Gbps on 21 Oct 2016
  - Attackers created a botnet from Internet of Things (IoT) using the Mirai IoT botnet malware
    - Had 100,000 malicious endpoints involved in the attack
- Geographic: 18 points of presence

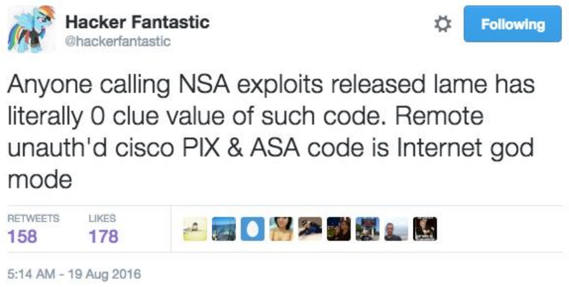


Map of areas most affected by Dyn attack, 11:45 a.m. EDT, October 21, 2016

- Systemic Attack
  - Amazon
  - Twitter
  - AirBnB
  - Pinterest
  - BBC
  - CNN
  - Spotify
  - Tumbler
  - Paypal
  - Netflix

Woolf, N. "DDoS attack that disrupted internet was largest of its kind in history, experts say". The Guardian. 26 October 2016. https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet
York, K. "Dyn Statement on 10/21/2016 DDoS Attack". Dyn. http://dyn.com/blog/dyn-statement-on-10212016-ddos-attack/

ShadowBrokers Release a Cyber Arsenal

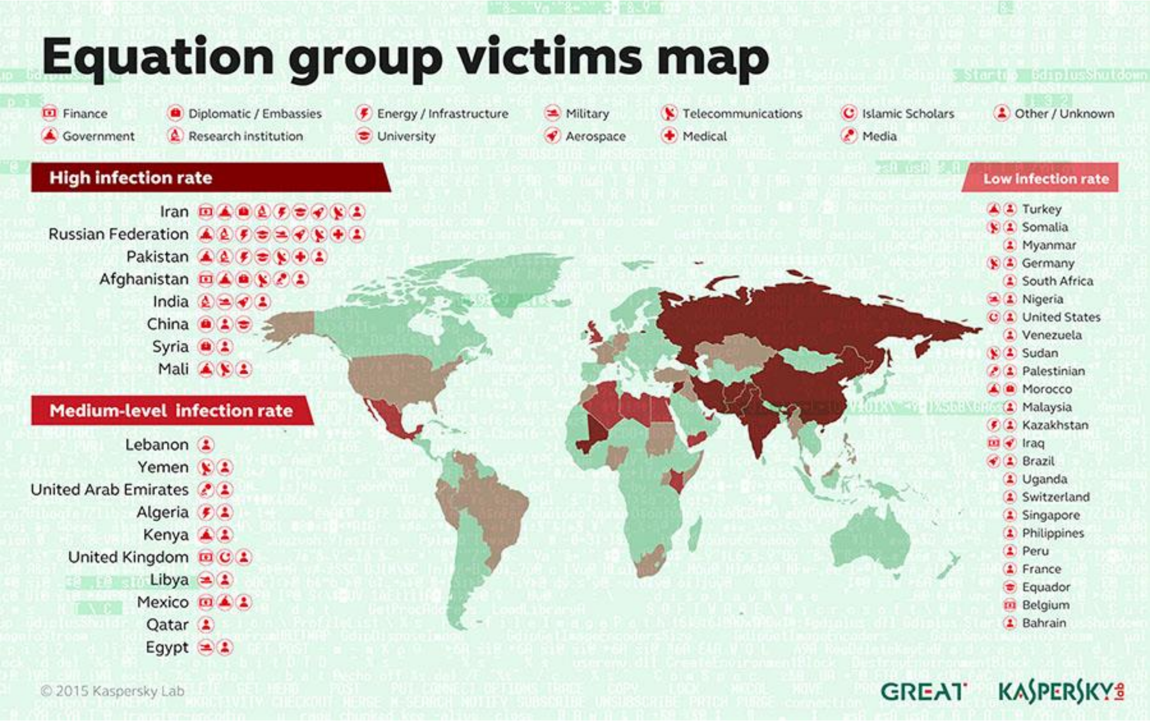


Hacker Fantastic
@hackerfantastic

Anyone calling NSA exploits released lame has literally 0 clue value of such code. Remote unauth'd cisco PIX & ASA code is Internet god mode

RETWEETS 158 LIKES 178

5:14 AM - 19 Aug 2016



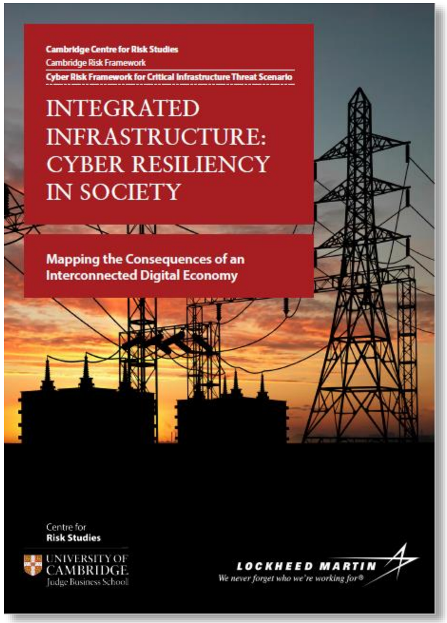
- On 13 August 2016 the ‘ShadowBrokers’ group released a showcase folder containing a set of cyber hacking weapons obtained from ‘Equation Group’
  - Obtained from the United States National Security Agency (NSA)
  - ShadowBrokers hacked the NSA or an insider leaked the materials
- The showcase folder released:
  - 15 exploits, 13 implants and 11 tools
  - Most notably a number of ‘zero day’ exploits to penetrate industry standard firewalls
- In October the Shadow Brokers leaked a further 300 files of IP addresses purportedly revealing NSA targeting and routing

References: Greenberg, 2016; Fox-Brewster, 2016; CERT, 2016.
Images: Tweet, NSA Picture, Victim map

Completed Cyber Research Projects 2016

- Integrated Infrastructure: Cyber Resiliency in Society
- Insurability of Cyber Catastrophe Risk – Assessment of PMLs
- Cyber Catastrophe Scenarios for Insurance Accumulation Management
- Cyber Terrorism Phase 1
- Cyber in Project Pandora and the Cambridge Global Risk Index 2017

Integrated Infrastructure: Cyber Resiliency in Society



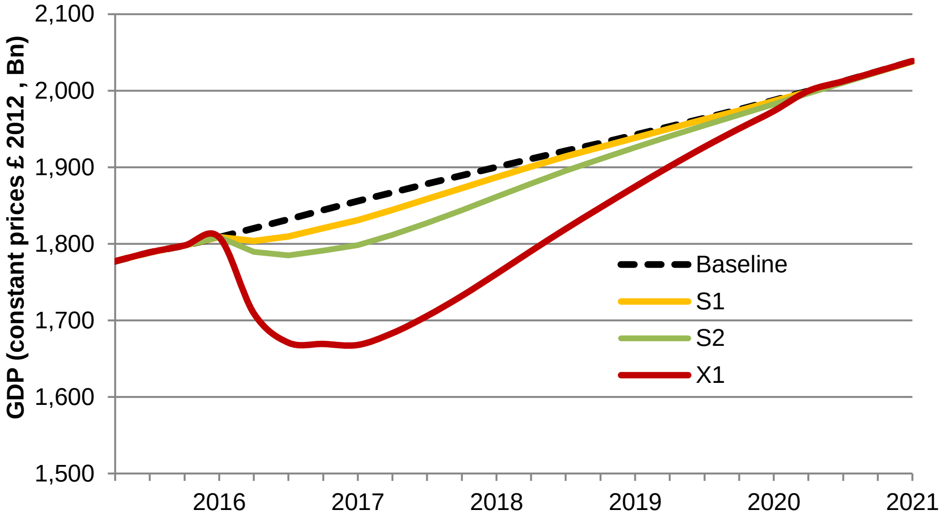
Cambridge Centre for Risk Studies
Cambridge Risk Framework
Cyber Risk Framework for Critical Infrastructure Threat Scenario

INTEGRATED INFRASTRUCTURE: CYBER RESILIENCY IN SOCIETY

Mapping the Consequences of an Interconnected Digital Economy

Centre for Risk Studies
UNIVERSITY OF CAMBRIDGE Judge Business School

LOCKHEED MARTIN
We never forget who we're working for®

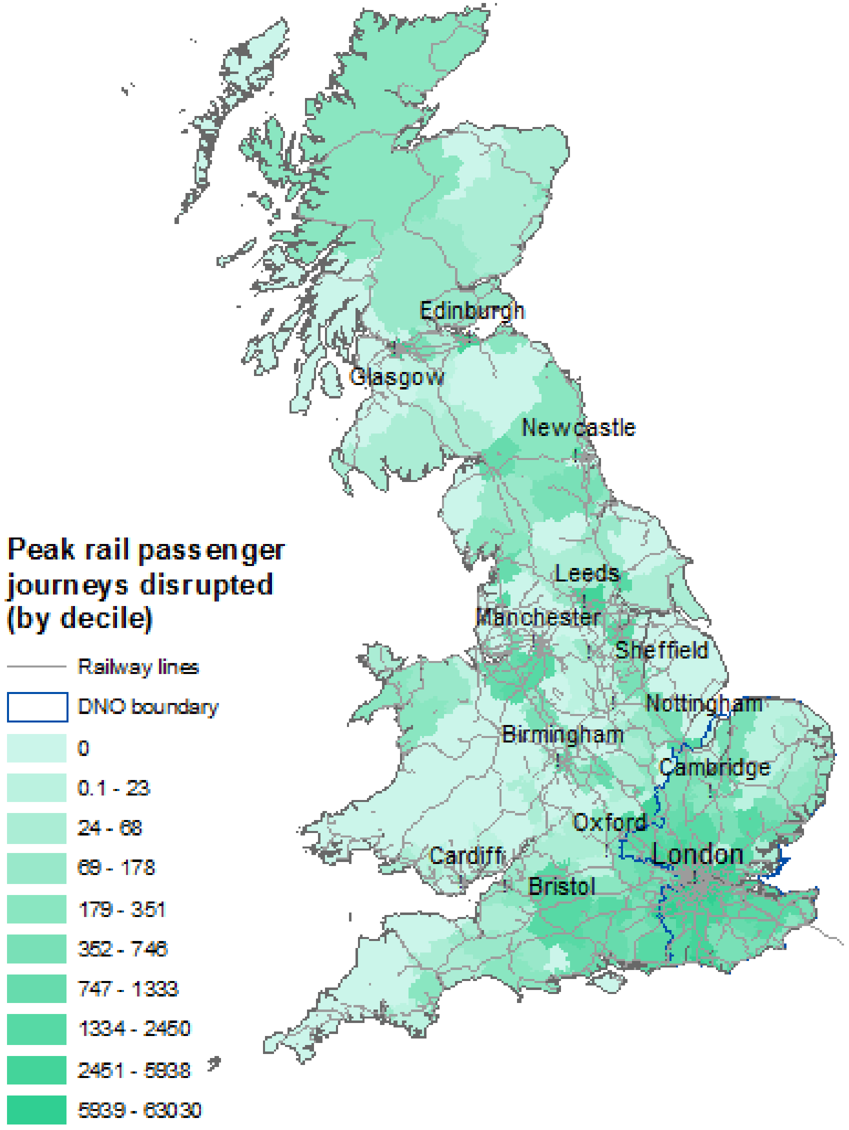


Domestic UK GDP@Risk under each scenario variant

Scenario Variants	Lost power (TWh)	Company (1 year direct) Sector Losses £ billion	Customer (1 year indirect) Sector Losses £ billion	GDP@Risk (5 Yr) impact on overall UK economy £ billion
S1	10.3	7.2	4.4	**49**
S2	19.8	18.0	10.9	**129**
X1	39.6	53.6	31.8	**442**

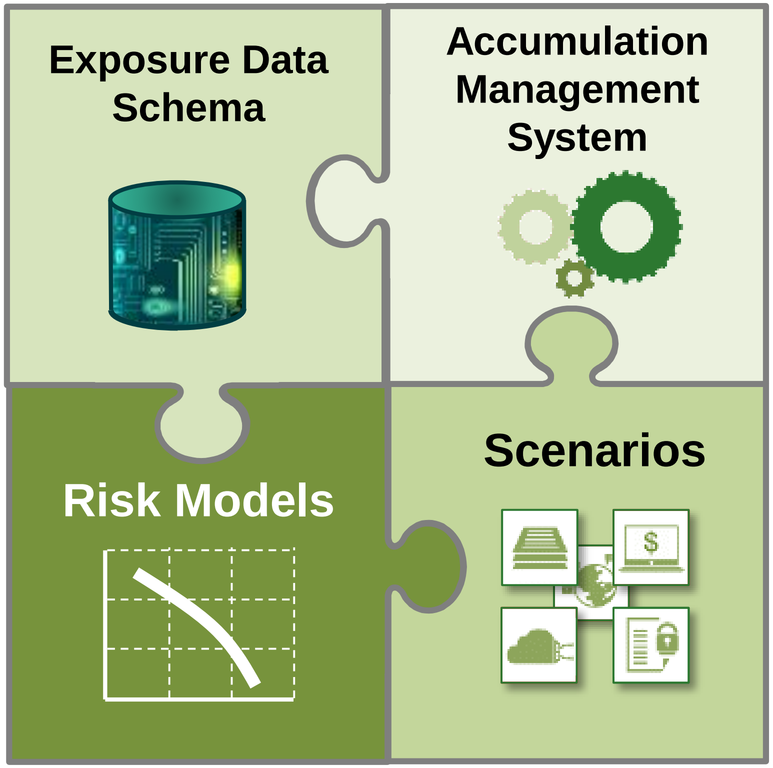
Integrated Infrastructure: Cyber Resiliency in Society

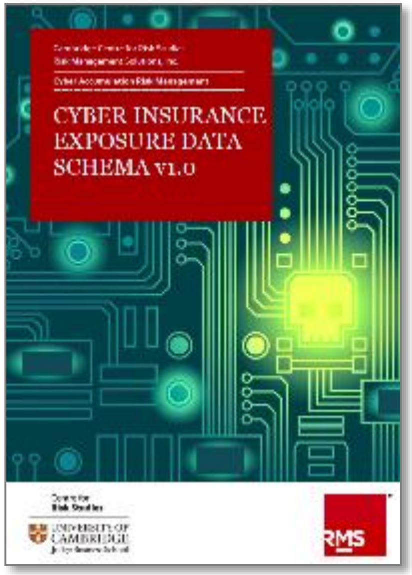
Railway customers disrupted



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

Cyber Catastrophe Scenarios for Insurance Accumulation Management – Assessment of PMLs




Cambridge Centre for Risk Studies
Risk Management Solutions, Inc.

Cyber Accumulation Risk Management

CYBER INSURANCE EXPOSURE DATA SCHEMA v1.0

Centre for Risk Studies

UNIVERSITY OF CAMBRIDGE
Judge Business School

RMS

Jan 2016
v1.0
First complete schema

Industry Organizations Supporting the Schema

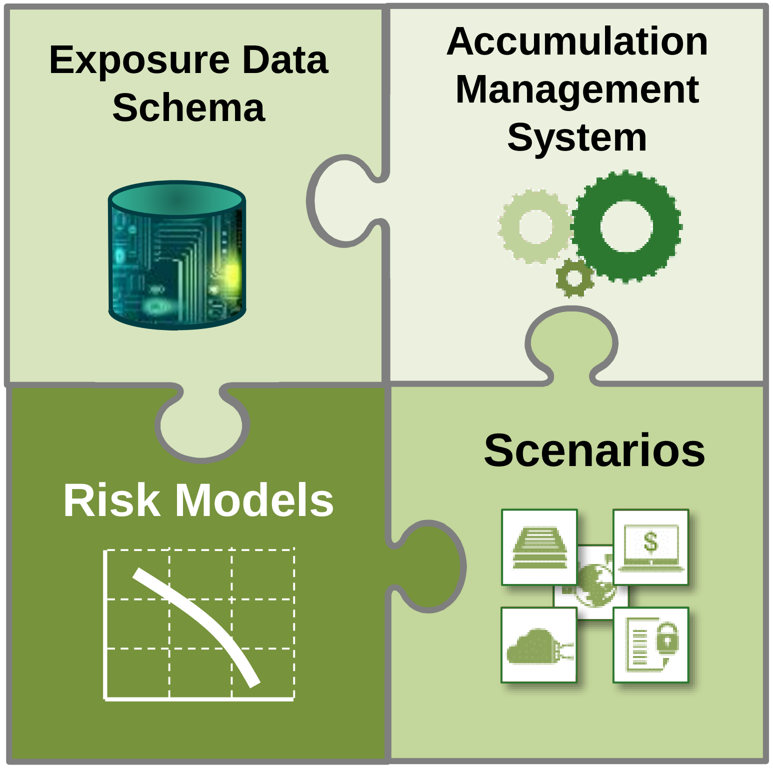
RAA
Reinsurance Association of America

LLOYD'S
Lloyd's

Lloyd's Market Association

CRO FORUM
Chief Risk Officer Forum

Cyber Catastrophe Scenarios for Insurance Accumulation Management – Assessment of PMLs



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

Data Exfiltration
('Leakomania')

Denial of Service Attack
('Mass DDoS')

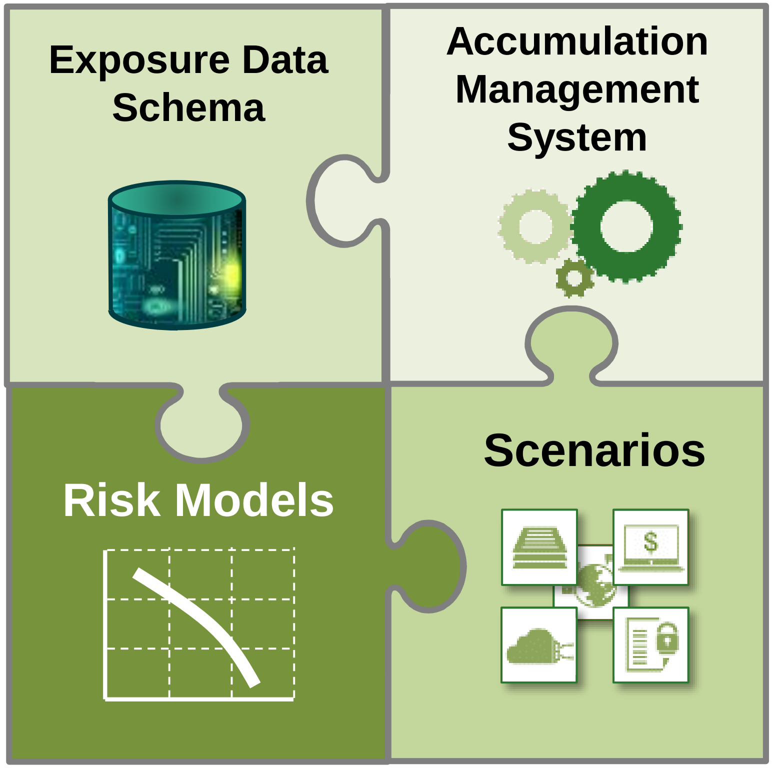
Cloud Service Provider Failure
('Cloud Compromise')

Cyber Heist
('Financial Theft')

Ransomware
('Extortion Spree')

ShadowBrokers
('ExtraBacon Exploited')

Cyber Catastrophe Scenarios for Insurance Accumulation Management – Assessment of PMLs



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')

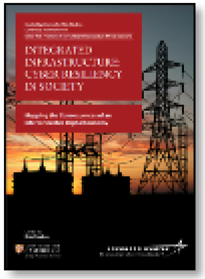
PCS-Triggered Explosions on Oil Rigs
('Phishing-Triggered Explosions')

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')

Business Blackout

The insurance implications of a cyber attack on the US power grid

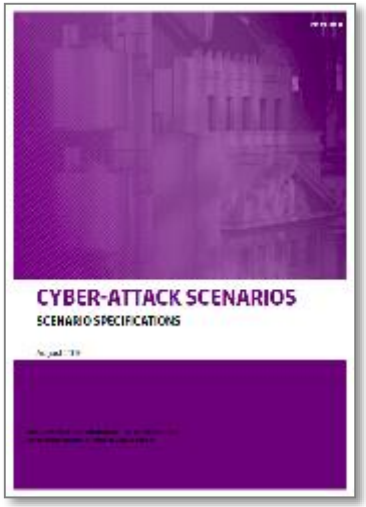

INTEGRATED INFRASTRUCTURE: CYBER RESILIENCY IN SOCIETY

CYBER TERRORISM: ASSESSMENT OF THE THREAT TO INSURANCE

UNIVERSITY OF CAMBRIDGE
Judge Business School

Centre for
Risk Studies

Lloyd’s Cyber RDS Scenarios


CYBER-ATTACK SCENARIOS

SCENARIO SPECIFICATIONS

	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

Business Blackout

The insurance implications of a cyber attack on the US power grid

Cyber Catastrophe Scenarios for Insurance Accumulation Management – Assessment of PMLs

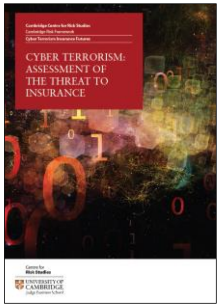
- Work started in June 2016 and continuing through 2018
  - Enhancements to RMS Cyber Accumulation Management System (v2.0)
    - Development of silent cyber scenarios
    - Reparameterize of affirmative scenarios
    - Cyber Risk Landscape 2017 report
  - Research to Support Development of Account-Specific Cyber Accumulation Analytics
    - Probabilistic cyber risk assessment modelling method review
    - Compilation of cyber data exfiltration incidences
    - Cyber account differentiation database

Cyber Terrorism Phase 1

- Report to be launched soon:
  - Several cyber terrorism scenario narratives
  - Cyber capabilities of various terrorist groups
  - Current methods of monitoring and defending against cyber terrorism
  - Insuring cyber terrorism

	Enabling				Disruptive				Destructive			
	Terror Group Website	Video & Social Media	Funding Ops Manuals	Encrypted Communications	Defacement of Websites	DDoS Website Take-down	Data Exfiltration Hack	Financial Cyber Heist	Sensor Spoofing	Control Engineering Compromise	Damaging/Disabling Infrastructure	Scaled Destruction on Multiple Targets
Al-Qaeda	◆	◆	♦	♦	♦							
Islamic State / United Cyber Caliphate	◆	◆	◆	♦	◆	♦	♦					
Nation State Cyber Unit E.g. Hezbollah Cyber Group	♦	♦	♦	♦	◆	◆	◆	♦				
Hacktivists Militant Destructive		♦	♦	♦	♦	♦						
Organised criminals				♦		◆	◆	♦				

	Mortality Rate	Physical Damage	Plausibility
2.3 Airplane Cyber Hijack	8	10	6
5.4 Eurostar Fire	7	10	7
9.1 Chemical Reactor Explosion	10	10	9
10.1 Ordnance Target	8	10	5


CYBER TERRORISM: ASSESSMENT OF THE THREAT TO INSURANCE

Cyber Terrorism Phase 2

- Current terrorism research activities
  - Develop structured approach to monitoring and producing a regular view on emerging cyber terrorism threats
    - Alerts and threat reports
  - Further cyber terrorism scenario development
  - Economic and societal loss estimation for cyber and non-cyber terrorism events

Cyber in Project Pandora

Cambridge Global Risk Index 2017

Cyber attack

- Cyber attack severities are increasing
  - Major recent cyber hacks have consistently broken previous records
    - Largest ever data exfiltration attacks (Yahoo 1 billion records and Mossack Fonseca 2.6 Tbytes)
    - Largest known attempted cyber bank theft (Lazarus SWIFT $1Bn attempt)
    - Largest Denial of Service attacks: 1,000 Gbps
    - Shadowbroker hack released NSA cyber weaponry to public
- Updated the Global Risk Index model to reflect increase in severity of cyber scenario

Cyber attack on Ukrainian power grid cut power to 225,000 people; Dec 2015

ShadowBroker cyber hack released NSA exploits to public; Aug 2016

Engagement, Outreach and Collaboration

- Engagement (UK, EU, US)
  - Industry (Insurance, Power, CyberGreen...)
  - Regulators (PRA, Lloyd’s, OfGen, NERC...)
  - Government (Cab Office, DECC, GCHQ, CPNI...)
- Outreach
  - Launch events
  - Conferences
  - Data standards
- Collaboration
  - Subject Matter Experts
  - Academia (ITRC...)
  - Consultants

Cyber Research Projects 2017

- Enhancements to RMS Cyber Accumulation Management System (v2.0)
- Research to Support Development of Account-Specific Cyber Accumulation Analytics
  - Hosting Cyber Probabilistic Modelling Workshop on 27 July 2017 in Cambridge
- Cyber Terrorism Phase 2
- Cyber in Project Pandora and the Cambridge Global Risk Index 2017

Centre for
Risk Studies

UNIVERSITY OF
CAMBRIDGE
Judge Business School