Cambridge Centre for Risk Studies

Advisory Board Research Showcase – 23 January 2018

Assessing Approaches to Cyber Terrorism

Centre for **Risk Studies**

UNIVERSITY OF CAMBRIDGE
Judge Business School

Tamara Evan
Research Assistant
Cambridge Centre for Risk Studies

Collaboration with Pool Re

- Established 1993 as a mutual insurer providing cover for terrorism damages on the UK mainland
- Collaboration with the Centre for Risk Studies began January 2016
- Since then, we have sought to better understand the cyber threat to the UK from extremist groups and the potential for systemic losses to UK industry from a developing terrorist peril, and provide useful metrics for communicating conclusions

The cyber terrorism threat entering 2018

- To date, there have been no known instances of destructive cyber terrorism causing physical damage
- Terrorism in the West during 2017 has been largely characterised by lone-wolf attackers linked via securitised cyber communications to a radicalised network

- The indication that counterterrorism and coalition military efforts have placed IS under increased organisational pressure suggest little movement in terms of IS' development of destructive cyber capabilities
- Given the collapse of IS territorial holdings and the diminishing physical 'caliphate' in the Levant, we must be aware of possible efforts to build a 'virtual caliphate' and an arsenal of cyber weaponry, spyware tools, disruptive malware, and related skillsets
- A potential for collaboration between IS and al-Qaeda could similarly reset goals to facilitate cyber development

The cyber terrorism threat through 2017

However, incidents of cyber crime remain newsworthy and frequent

Disruptive attacks

- **WannaCrypt**: 12 May 2017, 250,000 computers in 150 countries were locked by a virulent strain of ransomware, derived from exploits contained in the Shadowbrokers release
- **Reappearance of Shamoon malware**: January 2017, malware attack identical to 2012's Shamoon/Disstrack spotted in Saudi Arabian systems
- **NHS and US school website defacement by Team System Dz:** January and November 2017, visitors to 800 homepages were redirected to a Youtube video containing extremist statements and warnings. Content management system vendor School Desk was likely compromised.
- **DDoS attacks on Swedish transportation network and Danish Ministry of Immigration:** 28 September, and 11-12 October 2017, resulted in delayed and cancelled services on two consecutive days

Destructive attacks

- **Ukrainian substation attack**: 17 December 2016, suspicious hardware was found to have caused a 75 minute power outage in sub-zero temperatures affected Kiev and the surrounding area – a second repeat attack has not been reported for 2017
- **NotPetya**: June-July 2017, disk wiper affected 64 countries, mostly in Eastern Europe
- **IsraBye**: August 2017, an anti-Israeli disk wiper masquerading as ransomware found following the introduction of Israeli security measures on Jerusalem's al-Aqsa mosque
- **Continuing APT targeting of Western critical infrastructure**: summer 2017, minor discoveries incidents and phishing campaigns in the US, UK, Switzerland, Turkey targeting energy and CNI systems suggest intelligence gathering

Assessing the future threat

Monitoring group capability and identifying industry-specific cyber vulnerabilities

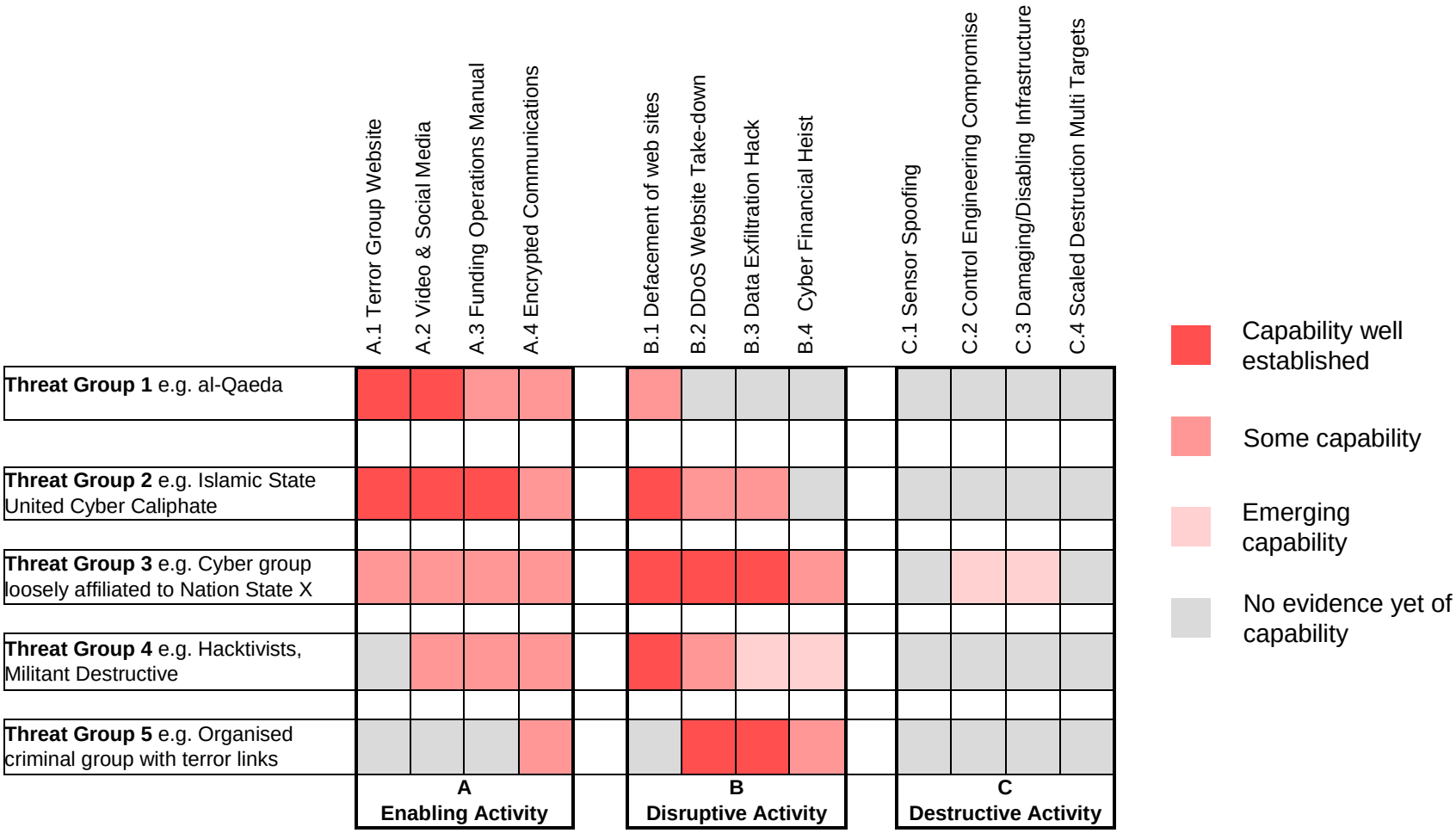
1. Monitoring of two key areas of capability development

- Capabilities of attributed terrorist threat groups
  - Tracking against the capability development matrix
- Evidence of destructive terrorism intent by unattributed threat actors
  - Successful or unsuccessful attempts to cause physical damage or human injury by remote digital attacks
  - From any threat actor, whatever attribution or unattributed

2. Creation with expert review of a longlist of low-probability scenarios

- Severities of outcome (damage impact, lives lost, spectacle grade)
- Difficulty of execution (logistical burden, plausibility)
- Ability to scale attack across multiple insureds
- Direct BI potential and overall economic impact

Cyber Capability Framework



Candidate ‘long-list’ of cyber terrorism scenarios

1. Real Estate

1.1 Boiler explosion
1.2 Smart Meter hijack
1.3 Manipulate sway control
1.4 Sprinkler systems
1.5 Halon Fire Suppressors
1.6 Door lock/Panic creation/Stampede
1.7 Electrical system overload/fire
1.8 Cooling system for server farms
1.9 Backup generator overload
1.10 Data centre battery power UPS
1.11 Alarm systems

2. Airports

2.1 Air traffic spoof creating airport crash
2.2 Fuel store fire
2.3 Airplane crash

3. Retail

3.1 Stampede/panic creation
3.2 Food security
3.3 Cold storage tampering

4. Construction

4.1 Crane hijack

5. Transport

5.1 Train/DLR crash
5.2 Tanker crash
5.3 Cargo explosion (chemical, etc.)
5.4 Eurostar fire

6. Power/Energy

6.1 Aurora style attack
6.2 Power Distribution Target
6.3. Oil Refinery Fire
6.4 Chemical spill
6.5 Turbine damage

7. Healthcare

7.1 Critical medical equipment
7.2 Prescription automation attack
7.3 HVAC systems target
7.4 Uninterrupted power systems attack
7.5 Pathogen release
7.6 Clean room attack

8. Pharmaceutical

8.1 Mass poisoning
8.2 Clean room sabotage

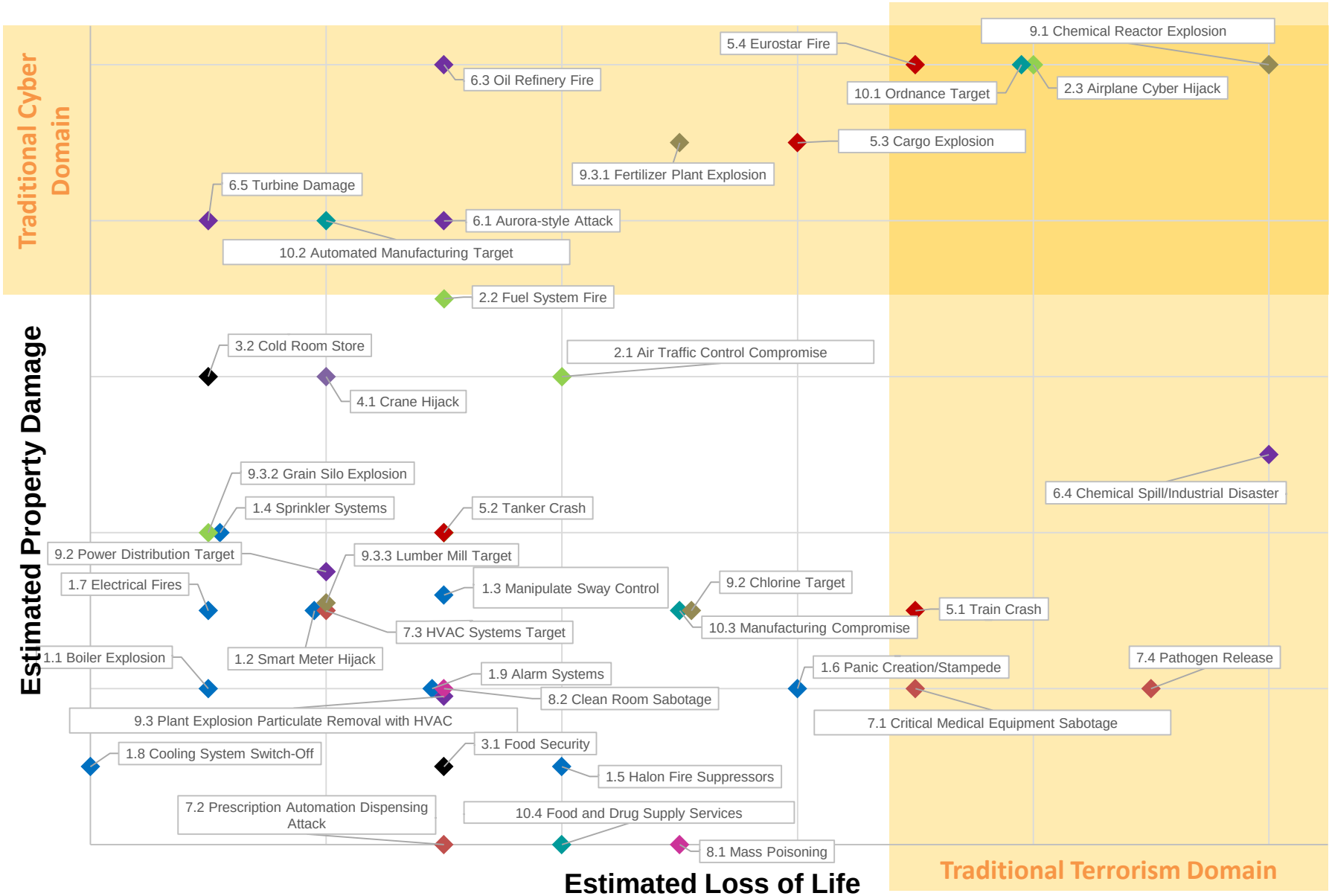
9. Chemical

9.1 Chemical Reactor Explosion
9.2 Chlorine Leak
9.3 Plant Particulate Removal with HVAC
9.3.1 Fertilizer Plant Explosion
9.3.2 Grain Silo Explosion
9.3.3 Lumber Mill Target

10. Aerospace

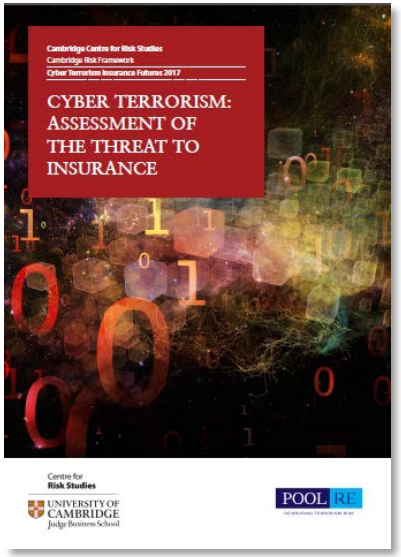
10.1 Ordnance target
10.2 Automated manufacturing target
10.3 Manufacturing spoof
10.4 Food and drug

Long-list qualitative mapping



Cambridge – Pool Re Collaboration

- 2016 Cyber Insurance Futures Report
  - Expert workshop
  - Report presented to Pool Re board mid-2016
  - Treasury granted permission August 2017
- 2017 Methodology
  - Monitoring capabilities of terrorist threat groups
    - Quarterly updates
  - Creation of low-probability cyber terrorism scenarios
    - Second expert workshop
    - In depth study of key loss processes
- Report: Cyber Terrorism: Assessment of the Threat to Insurance



November 28 Report and Schema Launch

2017 Scenario Design

"Big Bang“ or Bespoke attack	Systemic
2.1 Air traffic spoof creating airport crash	**1.1** Boiler explosion
2.2 Fuel store fire	**1.2** Smart Meter hijack
2.3 Airplane crash	**1.3** Manipulate sway control
4.1 Crane hijack	**1.4** Sprinkler systems
5.1 Train/DLR crash	**1.5** Halon Fire Suppressors
5.2 Tanker crash	**1.6** Door lock/Panic creation/Stampede
5.3 Cargo explosion (chemical, etc.)	**1.7** Electrical system overload/fire
5.4 Eurostar fire	**1.8** Cooling system for server farms
6.1 Aurora style attack	**1.9** Backup generator overload
6.3 Oil refinery fire	**1.10** Data centre battery power UPS
6.4 Chemical spill	**1.11** Alarm systems
6.5 Turbine damage	**6.2** Power distribution target
7.5 Pathogen release	**7.1** Critical medical equipment
7.6 Clean room attack	**7.2** Prescription automation attack
9.1 Chemical reactor explosion	**7.3** HVAC systems target
9.3.1-3 Particulate removal with HVAC	**7.4** Uninterrupted power systems attack
10.1 Ordnance target	**10.3** Manufacturing spoof (chemical, pharma, aerospace)
10.2 Automated manufacturing target	**10.4** Food and drug

2017 Scenario Design

"Big Bang“ or Bespoke attack	Systemic
2.1 Air traffic spoof creating airport crash	**1.1** Boiler explosion
2.2 Fuel store fire	**1.2** Smart Meter hijack
2.3 Airplane crash	**1.3** Manipulate sway control
4.1 Crane hijack	**1.4** Sprinkler systems
5.1 Train/DLR crash	**1.5** Halon Fire Suppressors
5.2 Tanker crash	**1.6** Door lock/Panic creation/Stampede
5.3 Cargo explosion (chemical, etc.)	**1.7** Electrical system overload/fire
5.4 Eurostar fire	**1.8** Cooling system for server farms
6.1 Aurora style attack	**1.9** Backup generator overload
6.3 Oil refinery fire	**1.10** Data centre battery power UPS
6.4 Chemical spill	**1.11** Alarm systems
6.5 Turbine damage	**6.2** Power distribution target
7.5 Pathogen release	**7.1** Critical medical equipment
7.6 Clean room attack	**7.2** Prescription automation attack
9.1 Chemical reactor explosion	**7.3** HVAC systems target
9.3.1-3 Particulate removal with HVAC	**7.4** Uninterrupted power systems attack
10.1 Ordnance target	**10.3** Manufacturing spoof (chemical, pharma, aerospace)
10.2 Automated manufacturing target	**10.4** Food and drug

2017 Scenario Design

Major bespoke cyber attack: Chemical explosion/fire at major facility

A chemical fire is caused by a cyber attack at a major facility, causing wide-scale damage, evacuations and extended BI in surrounding areas

Systemic high-frequency cyber attack: Commercial property fires

A lithium battery firmware hack causes a number of fires to break out overnight in office buildings, causing significant property damage

Scenario: Cyber-Induced Explosion in a Major Chemical Processing Facility

‘Fuel bomb’ leak at major chemical facility
(Chemical reactor explosion)

	Mortality Rate	Physical Damage	Media Impact	Plausibility	Scalability	Direct BI Potential	Overall Economic Impact
9.1 Chemical Reactor Explosion	10	10	10	9	2	3	1

	Standard Scenario (S1)	Scenario Variant (S2)	Extreme Variant (X1)
Variant Profile Description	A significant fire causes physical damage at the facility	A major explosion at the facility with blast radius with 2km debris scatter	Chemical explosion with blast radius impacts key facility operations with 2km debris scatter
Loss of Affected Site (Property)	50%	50%	Write-off (100%)
Loss of Affected Site (Contents)	50%	50%	50%
Surrounding Area of Business Affected	Facility only	2km radius	2km radius
Total Loss Value	**£ 507m**	**£ 625m**	**£ 1,132m**

Scenario: Cyber-Induced Fires in Commercial Office Buildings

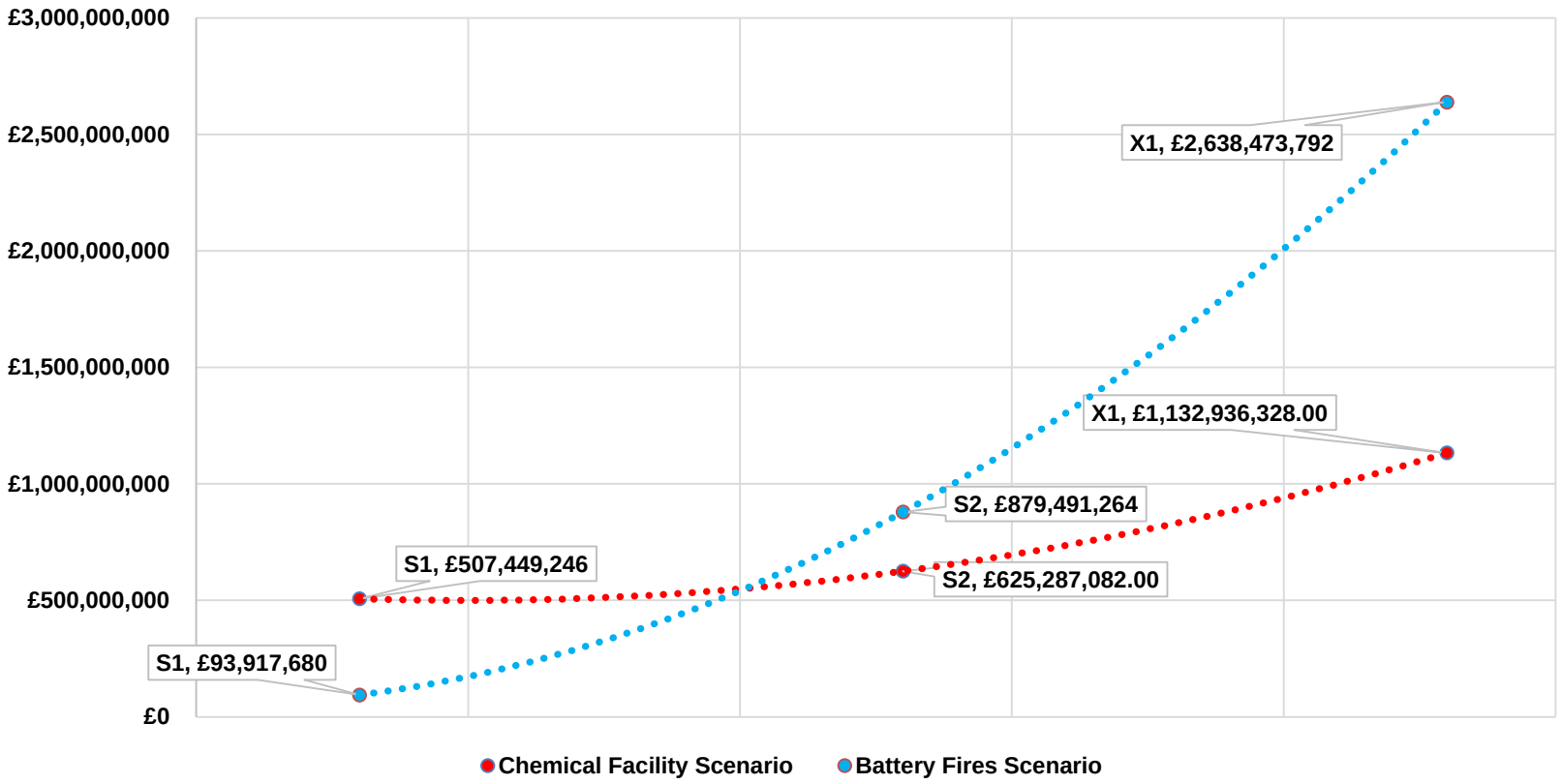
Cyber-Induced Fires in Commercial Office Buildings
(Lithium battery fire induction)

	Mortality Rate	Physical Damage	Media Impact	Plausibility	Scalability	Direct BI Potential	Overall Economic Impact
1.7 Electrical Fires	1	6	6	3	8	3	2

	Standard Scenario (S1)	Scenario Variant (S2)	Extreme Variant (X1)
Variant Profile Description	In cases of a single laptop's destruction (LFD), 20% of affected businesses claim BI for one day. Other Fire damage variations affect 50% of Businesses.	In cases of a single laptop's destruction (LFD), 50% of affected businesses claim BI for one day. Other fire damage variations affect 75% of Businesses.	In cases of a single laptop's destruction (LFD), 75% of affected businesses claim BI for one day. Other fire damage variations affect 100% of Businesses.
Business Interruption LF3 – LF5	50%	75%	100%
Rate of workplace device ignition	0.11%	1.04%	3.12%
Total Loss Value	**£93m**	**£879m**	**£2,638m**

Loss Estimate Comparison

	Standard Scenario (S1)	Scenario Variant (S2)	Extreme Variant (X1)
Chemical Facility Explosion Scenario	£507,449,246	£ 625,287,082	£ 1,132,736,328
Battery Fires Scenario	£93,917,680	£879,491,264	£2,638,473,792



Next steps: 2018-19

- Review and revise the scenario long-list for 2018
- Continued monitoring of the threat, known actors, and areas of potential vulnerability
  - 2018 Meltdown and Spectre chip vulnerabilities
- Building of a cyber terrorism ‘tool-kit’ for systemic loss modelling
- Producing a data schema for improved insured portfolios
  - How an insurer can promote better cyber hygiene, loss mitigations, and responsible incident reporting across insureds