



Presentation to the Cyber Insurance Summit Switzerland

11 December 2024

Agenda

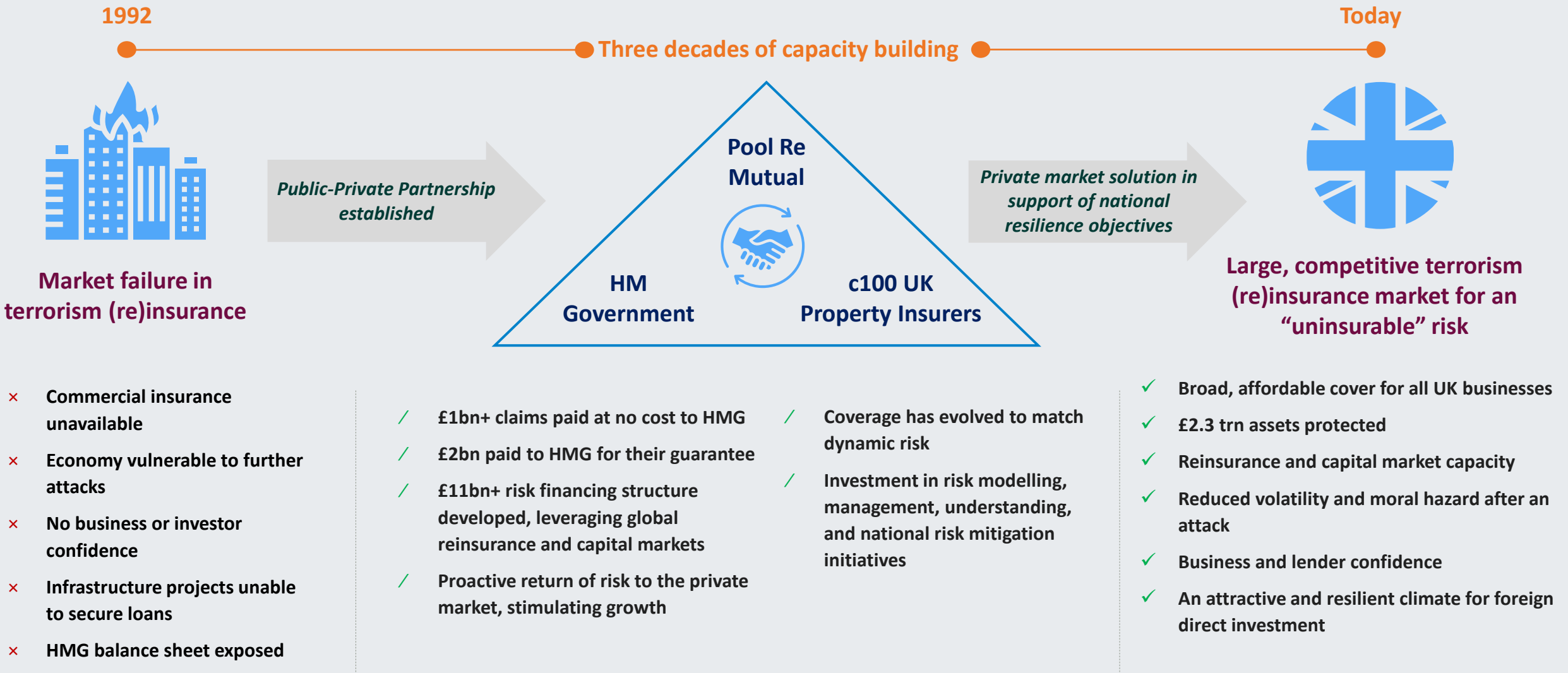


- 1 General Framework of Pool Re
- 2 Specific Considerations for Cyber Risk

1. General Framework of Pool Re



Pool Re exists to correct market failure, providing confidence and resilience to the national economy whilst supporting and returning risk to the private insurance market.



- × Commercial insurance unavailable
- × Economy vulnerable to further attacks
- × No business or investor confidence
- × Infrastructure projects unable to secure loans
- × HMG balance sheet exposed

- ✓ £1bn+ claims paid at no cost to HMG
- ✓ £2bn paid to HMG for their guarantee
- ✓ £11bn+ risk financing structure developed, leveraging global reinsurance and capital markets
- ✓ Proactive return of risk to the private market, stimulating growth

- ✓ Coverage has evolved to match dynamic risk
- ✓ Investment in risk modelling, management, understanding, and national risk mitigation initiatives

- ✓ Broad, affordable cover for all UK businesses
- ✓ £2.3 trn assets protected
- ✓ Reinsurance and capital market capacity
- ✓ Reduced volatility and moral hazard after an attack
- ✓ Business and lender confidence
- ✓ An attractive and resilient climate for foreign direct investment

Core Stakeholders



Insurer Members

- Pool Re is a **Member-owned mutual**; it is “not for profit”
- **Only Members may cede to the pool**; 100% GWP is generated by the Membership
- Pool’s membership comprises **nearly all regulated UK property insurers** who retain the primary terrorism risk – approximately 90% of the UK commercial terrorism market
- **All funds belong to the Members**



HM Treasury

- HMT is Pool Re’s sponsoring department in Government, **underpinning the scheme with an unlimited guarantee**
- Pool Re is an **Arm’s Length Body of HM Treasury**
- As an ALB, Pool Re has to comply with a number of policies and guidelines (e.g. Managing Public Money, Public Procurement etc) and is **audited by the National Audit Office**
- Annually, HMT receive **50% of Pool Re’s GWP + 25% of distributable profit**
- **5-year Review cycle to** review the scheme’s function in the market and strategy

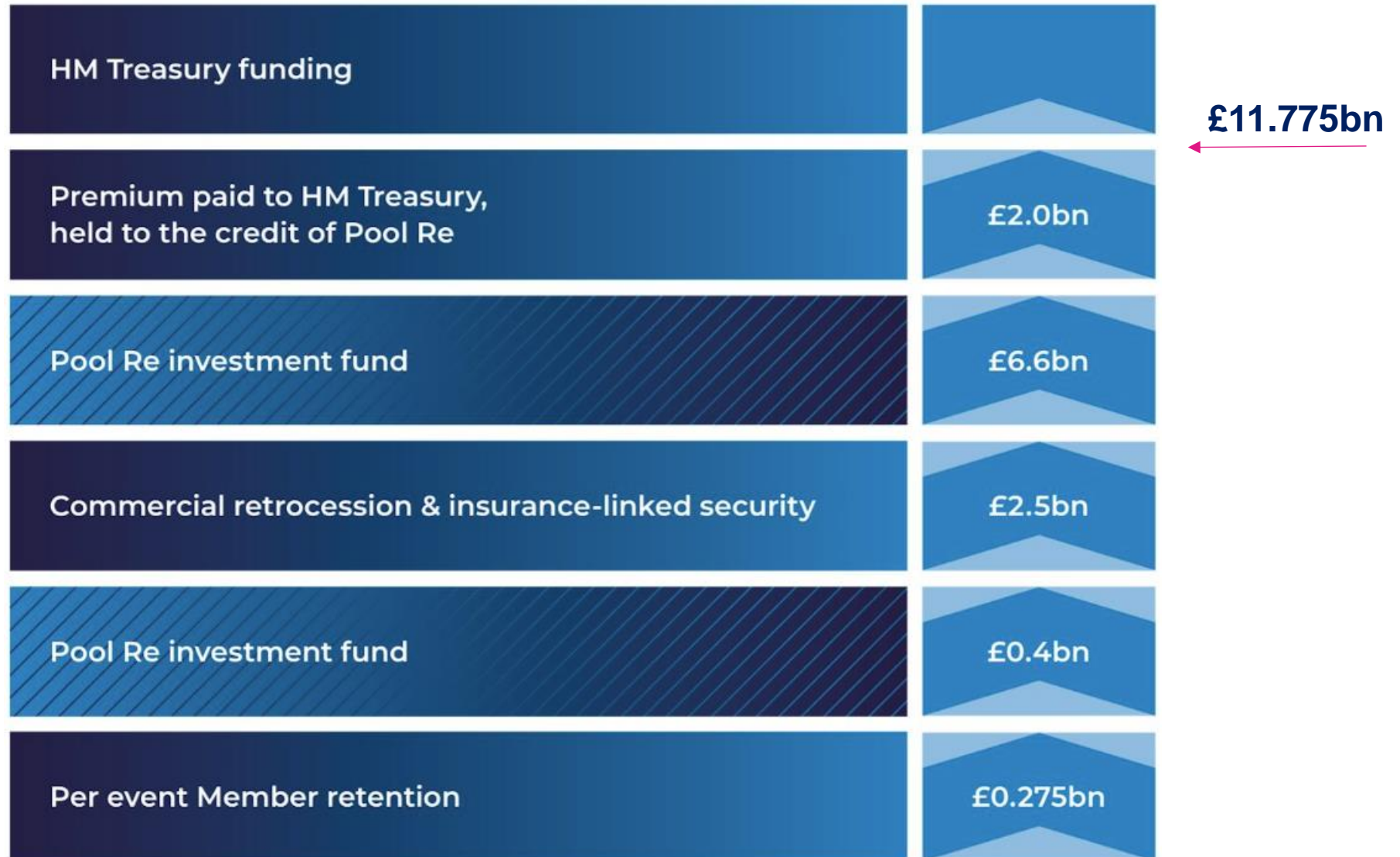


UK Regulatory Authorities

- Pool Re is **dual regulated** by the PRA and FCA
- The **PRA is the principal regulator**
- Pool Re is a Large Non- Directive firm – i.e. **the Solvency II Directive does not apply** and there is **no regulatory capital requirement**, in each case through waiver



Scheme Resilience in 2024



Features of Pool Re's current model provide certainty and value for the pool's wide spectrum of membership



- 1. Solvency:** Members of Pool Re are guaranteed solvency for any legitimate claims arising from a certified act of terrorism, and are not required to hold the vast capital reserves that Solvency II regulation would require in Pool Re's absence.
- 2. Availability:** Pool Re cover is accessible through any of the scheme's Members, who together constitute the vast majority of property insurers in the UK market.
- 3. Guaranteed acceptance:** Membership of Pool Re is open to any authorised insurer. Cover and terms are not restricted by geographic area or risk profile.
- 4. Capacity:** Pool Re is backed by an uncapped HMT guarantee, underpinning £2.3 trillion of UK assets. After even a series of catastrophic events, Members can be certain of immediate liquidity, and continued reinsurance cover at an affordable rate, something that would not otherwise be available.
- 5. Claims transparency:** Claims are handled by the underlying property insurer within a pre-defined protocol. There is an agreed process for the certification of an event as one of terrorism, with a binding tribunal process to resolve disputes.
- 6. Breadth of cover:** Terrorism damage caused by CBRN means is included as standard. We also cover acts of terrorism where damage is caused by a remote digital trigger, and in February 2019 the scheme was widened to include non-damage BI.

Key Rules which underpin the current Scheme and which Members must follow



1. *Make cover available*

- × Upon request by a policyholder, a Member must offer terrorism cover

2. *Cede all Business*

- × Members must cede all eligible terrorism risks to the scheme and cannot retain policies for their own account

3. *All or Nothing*

- × Policyholders must buy terrorism cover for all eligible property and cannot select certain risks only

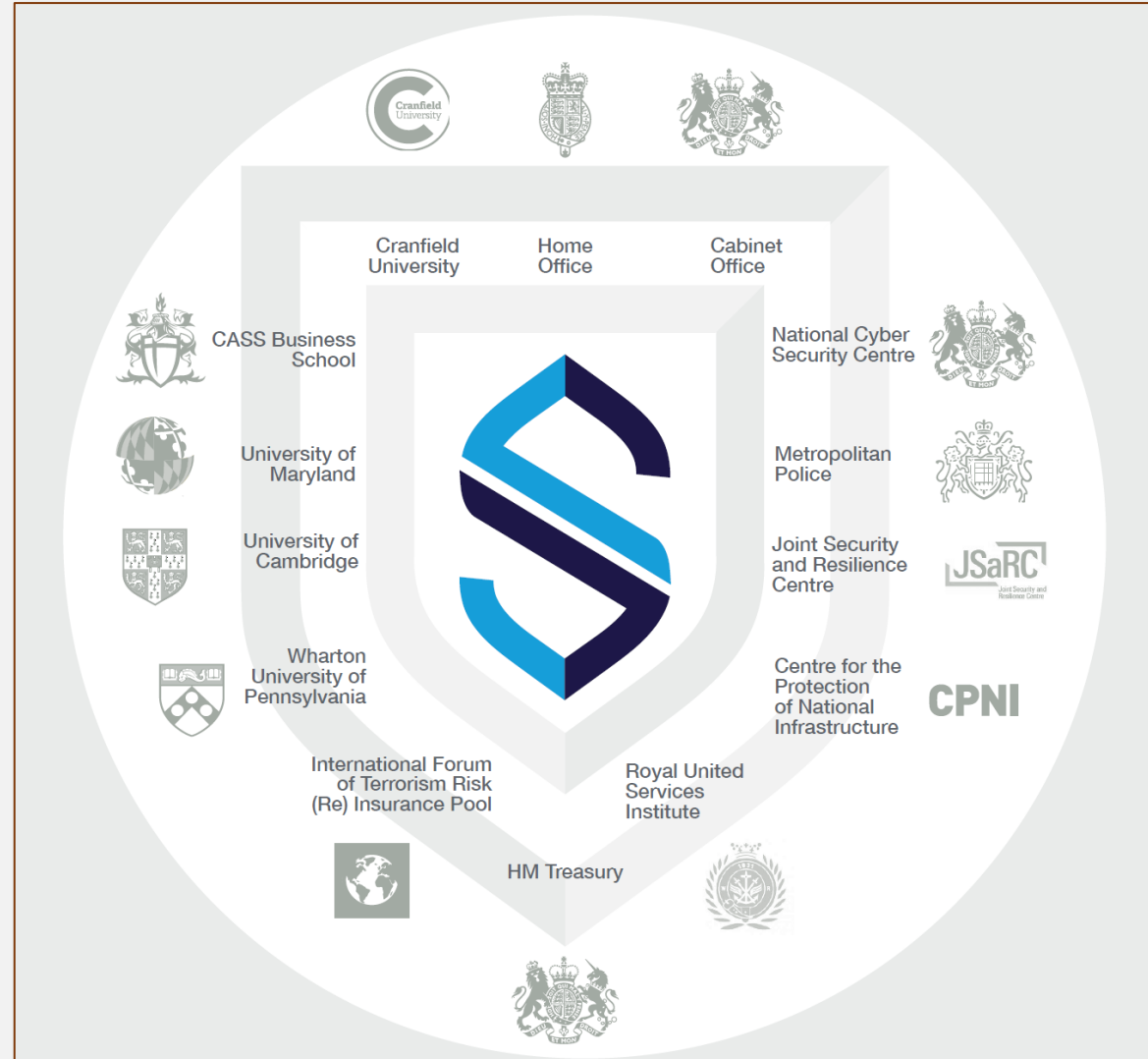
4. *Scope of Cover*

- × Members must offer policyholders the same cover as they receive from Pool Re. They cannot offer conventional and remove non-conventional



Risk Mitigation: Pool Re *Solutions*

We are able to use our unique market position to invest in partnerships and protective security initiatives with academia, risk specialists, and public agencies to understand and mitigate terrorism risk.





Pool Re Solutions: Capabilities

Threat Awareness

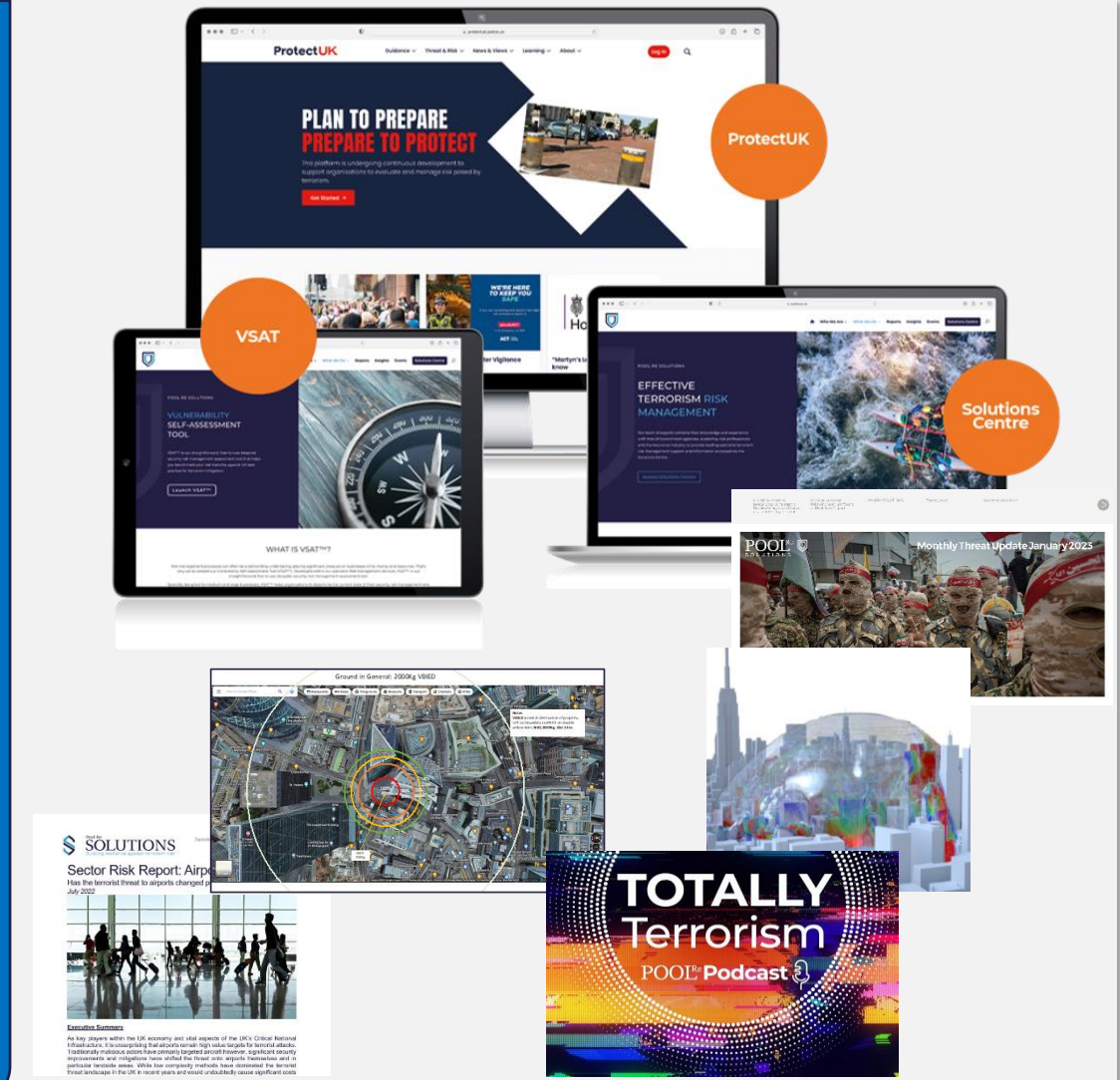
Providing credible analysis and understanding of the terrorism threat:

- ✓ Blogs
- ✓ Monthly Threat Bulletin
- ✓ Deep-Dive Reports and Thought Leadership
- ✓ Bespoke analysis
- ✓ Threat Education
- ✓ Credible Scenario development

Risk Management

Providing expert advice on managing the threat:

- ✓ Free-to-use advice
- ✓ Vulnerability Self-Assessment Tool (VSAT)
- ✓ Threat, Vulnerability, Risk Assessments (TVRAs)
- ✓ Probable Maximum Loss Studies (PMLs)
- ✓ Policy Reviews
- ✓ Training and exercises



Catalogue of Government Pools: World Regional View



Peril	Africa	Americas	Asia	Europe	Oceania	Global**	Total
Agricultural Pool	-	-	-	2	-	-	2
Drought	17	8	5	1	-	-	31
Earthquake	-	5	10	1	1	-	17
Environmental Liability Risks Pool	-	-	-	3	-	-	3
Flood	3	8	12	2	1	-	26
Motor	-	-	2	2	-	-	4
Multi-peril	-	6	-	-	-	-	6
Natural Catastrophe Pool	15	31	21	13	1	3	84
Nuclear	2	7	4	14	1	-	28
Other*	38	57	60	35	1	-	191
Terrorism	3	2	4	10	1	-	20
Wind	-	28	6	5	-	-	39
Total	78	152	124	88	6	3	451

*Other Perils include Agricultural Insurance and Reinsurance, War, Energy, Medical, Aviation, Cargo, Engineering, Oil, Gas exploration, Micro Insurance, Marine, Loan Guarantee, Motor, Employers Liability, Disaster Micro Insurance Pools, Pools for Enterprises involved in hazardous activities.

**Global pools include Global Climate Insurance Pool (initiative put forward by MCII (Munich Climate Insurance Initiative); Global Index Reinsurance Facility (GIRIF) managed by the World Bank

2. Specific Considerations for Cyber Risk





The cyber protection gap we are seeking to address is largely a result of limited demand for cyber cover and insufficient capacity for systemic events

Demand-side challenges primarily affecting SMEs

Businesses do not understand or prioritise cyber risk, and choose not to buy cover

Companies cannot afford cover

Many companies **deprioritise cyber as they cannot afford it alongside traditional P&C lines** (particularly as these lines have also become more expensive since 2020), and do not consider cyber risk as critical

Companies underestimate their exposure

Companies **often underestimate their exposure to cyber risk**, particularly amongst SMEs, meaning they do not purchase the level of coverage required when they should (time inconsistency)

Companies don't meet insurer requirements

Insurers typically require a **minimum level of risk management** to provide coverage, however the costs and efforts associated with this are beyond what some companies feel is appropriate

Supply-side challenges primarily affecting larger corporates

The nature of the risk means the market is unable to accurately size and assess cyber risk

Claims complexity means event response can be slow

Assessment of **claims is a complex and litigious exercise**, which delays pay outs, inflates costs, and potentially results in negative externalities if liquidity does not get to companies fast enough

Prices are high due to the complexity in modelling risk

(Re)insurers have **difficulties in modelling** due to information asymmetry, a lack of historical claims data, and the inherent characteristics and dynamic nature of cyber risk that makes prediction difficult

Purchasing processes are not standardised across insurers

Application processes tend to be complicated (especially for SMEs) and lack standardisation across insurers, requiring potential policyholders to invest significant time and resources to get coverage

There is insufficient private capacity to cover large-scale systemic events

Companies cannot obtain cover proportionate to the cyber threat

Insurers are **forced to exclude systemic cyber events from coverage** (including state actions and warfare, and/or attacks on CNI), leaving the UK economy significantly exposed in the event that a catastrophic cyber-attack that damages multiple organisations simultaneously

⚠️ Uninsurable risk that insurers cannot be expected to cover

We proposed a risk pooling solution, as part of broader pre-emptive efforts, to strengthen the UK's overall cyber resilience



1 What is the ambition?

Narrow the cyber protection gap to strengthen the UK's resilience

2 What role will the risk pooling solution play?

 Cover large-scale systemic cyber events that could inflict catastrophic damage on society and the economy

 Provide cover to 'unsophisticated' businesses via mandatory tariff on insurance policies

 Provide cover to 'sophisticated' clients via premium contribution from cyber policies

3 How can the risk pooling solution operate?

Funding the scheme

Upfront seed funding required, with ongoing funding from tariff, premium and retrocession

Sharing the risk

Layered approach spreading the risk between policyholders and the reinsurance market, with government a last resort

Defining an event

Simplified declaration and classification system based on scale of event

Paying a claimant

Predetermined rapid full payout for unsophisticated firms, with payouts akin to industry norms for sophisticated

4 What are other considerations?



Administration and oversight



Underwriting, claims and other capabilities



Broader responsibilities for risk mitigation to reduce overall cyber risk

We set out five success criteria for the scheme that underpin the ambition to narrow the cyber protection gap



NARROW THE CYBER PROTECTION GAP TO STRENGTHEN THE UK'S RESILIENCE



Reduce the UK's cyber risk exposure by promoting business resilience

- The scheme should promote resilience at a business and ultimately a society level to reduce overall cyber risk exposure
- The scheme can do this by using **risk-based pricing to encourage better behaviour**, insisting **policyholders implement minimum security measures**, and **investing surplus funds in broader ex-ante risk mitigation initiatives** like education



Crowd in private insurance, encouraging sustainable cyber market growth

- The scheme should **only address the failure of the market to cover systemic risks**, which are uninsurable by the private market due to their widespread, unpredictable nature.
- It should **not attempt to cover any risks the private market can feasibly address alone**
- The scheme should act as a buffer for the private market, facilitating and **supporting its growth**, and should be dynamic enough to **reflect increasing private market capacity**



Improve coverage accessibility, affordability and comprehensiveness

- The scheme should **increase the number of overall businesses that hold cyber insurance** by offering cover that is both accessible and affordable
- The scheme would also achieve this through improvements to the comprehensiveness of the cover, given it would cover the systemic risks currently excluded by the private market due to the fear of risk aggregation and scale of potential losses



Provide targeted, certain and rapid liquidity to businesses when they need it

- Insurance is a more effective way of responding to a systemic event than ex-post solutions
- The scheme should be **designed to ensure liquidity is provided to businesses that need it immediately**, reducing drag-on effects and avoiding unnecessary bankruptcies and economic disruption



Adequately remunerate government for the risk and limit balance sheet impact

- *The government has outlined a framework for contingent liabilities and achieving value for money*
- *The scheme should align to this framework, providing fair compensation for the risk government would bear*
- *As an example, Pool Re pays a dividend to HMT, funded by its premium receipts and investment income*

Relevant when making case to government

We proposed the implementation of a reinsurance scheme structure for larger and more sophisticated firms, and a compensation scheme for smaller and typically less sophisticated firms




Compensation Scheme	Reinsurance Scheme
Low insurance take up & limits for SMEs means a mandatory tariff safety net provides a better base	Most cyber insurance is purchased here, allowing for a “Pool-Re” like design to function


Design component	Proposed approach	
Business model	Safety net structure	Reinsurance scheme
Participation obligation	Mandatory (insurer-administered)	Voluntary for insurers to participate, with obligation to cede all
Coverage	Systemic events (impact-based)	Systemic events (impact-based)
BAU funding	Tariff on cyber-adjacent P&C lines of business	Cyber premium driven reinsurance contribution
Firm eligibility	Below turnover and cyber limit thresholds	Above turnover or cyber limit thresholds
Claims triggers	Multiple impact-focussed parametric-like triggers	Multiple impact-focussed parametric-like triggers
Limits of payout	Predetermined payouts based on tariff value	Per firm limits
Payout speed	Rapid full payout	Driven by industry norms


These are separable but have been put together to support the migration from the unsophisticated to the sophisticated scheme


Four points of broad consensus around targeted intervention have emerged from the industry consultation to date



1  **Systemic cyber risk is a real problem that will only increase, rather than diminish**

2  **Systemic cyber risk is a problem for the insurance industry and should be addressed in a co-ordinated way for the sake of its reputation and relevance**

3  **The chance to think about these issues and the design of a potential partnership with government before a catastrophic event is welcome**

4  **Systemic cyber risk can only be addressed meaningfully through some form of partnership with the state**

Insurance industry participants were supportive of the concept of a cyber reinsurance risk scheme for sophisticated clients



Participants saw this as a feasible and palatable solution, and were supportive on two key conditions...

... and agreed that outstanding design questions were dependent on testing Government appetite for intervention

01



Insurer participation is voluntary

01

Clarify definition of a cyber event – propose a broad definition of “a loss arising from a failure of computer systems”

02



The scheme does not crowd out the private market

02

Clarify scope of cover – decision for primary carriers to decide through ABI working group participation

03

Clarify attachment point of RI Scheme – intended to start at the 1 in 50 RP and increase over time

However, insurance industry participants raised some reservations regarding the compensation scheme's design



The cost that a compulsory safety net tariff would impose on small businesses in the current economic climate

01



There is no obvious P&L upside for insurers in administering the safety net, but potentially significant administrative cost and hassle

02



The possibility that a mandatory compensation safety net would make it harder for insurers to sell cyber products to SME clients

03



04

A tariff on adjacent P&C lines may complicate and dilute existing wordings with the inclusion of a cyber element

07

There may be events which trigger the safety net, and cause payouts to a large number of firms that were not affected



06

There may be difficulties delineating between sophisticated and unsophisticated businesses



05

The risk of policyholder complaints if cyber claims are denied because the event has not been systemic enough to trigger the safety net



In response to reservations on the compensation scheme, 3 key scope questions emerged



1

Do we keep the compensation scheme?

Despite reservations, the view was to retain the Compensation Scheme proposal for now, given that:

- It is an effective way to inject liquidity into the economy rapidly following an event
- It is preferable to HMG hastily assembling a scheme in the aftermath of a cat event leading to avoidable delay, multiplier effects, and fraud.
- SMEs make up 99% of UK businesses and are especially vulnerable to an event which prevents them trading for even a few weeks.
- To propose a scheme solely for larger corporates would be to ignore the SME constituency and be potentially unpalatable politically
- **Note that the compensation scheme is not intrinsically connected to the reinsurance scheme, and that one can operate without the other.**



2

If we do keep it, do we fund the solution via a levy or through IPT?

The preference was to fund the Compensation Scheme through IPT (ideally without a rise in the current rate) and introduce an administration fee

Doing so would address concerns around:

- Insurers needing to adjudicate on whether policyholders are 'sophisticated or 'unsophisticated'
- Attaching a tariff to adjacent P&C lines
- **Note that there is precedent in ring-fencing a portion of IPT proceeds for a specific resilience objective, namely investment in flood defences in 2016.**



3

Do we opt for impact-based or more complex triggers?

The benefits of a single parametric trigger as originally proposed include:

- Simplicity
- Speed of payouts

However, in the interests of fairness of payout distribution, it is proposed to introduce a double trigger design to mitigate the risk of overpayments to large numbers of firms who are unaffected by an event.

The first trigger would relate to the magnitude of the event, and the second would require some form of loss to be experienced by firms.

In addition to the two schemes proposed, other complementary initiatives emerged from the Consultation to promote national cyber resilience and address the supply and demand side problems identified



Additional solutions are not mutually exclusive, and several can be leveraged to support SMEs (including alongside the safety net)

01

Government procurement mandate

02

Bank loan condition precedent

03

Regulatory pressure

04

Education / awareness campaigns

05

Grants and bursaries to address significant cyber risks (public/ private)

06

Enhance, consolidate and promote best practice cyber standards

07

Link standards directly to the underwriting process

08

HMG co-ordination of finite incident response capacity to improve business' access to expertise following a major event

09

Use of insurance industry's claims-payment infrastructure to inject liquidity into the economy in the absence of any pre-funded scheme

In the extreme, compulsory cover of catastrophic cyber cover would provide a solution, though no appetite was expressed for this during the Consultation



Next Steps

- 1 It was agreed that the proposals represented, in principle, a positive step in helping to address a material problem for the industry and the economy.
- 2 Whilst further discussion would be required to agree the final terms of any public-private scheme, it was agreed that there was a window of opportunity to engage with the incoming Government to discern their appetite for engaging with the industry on such a partnership.
- 3 Accordingly, it was agreed that the industry should engage with HMG to discuss the possibility of establishing a public-private partnership in relation to catastrophic cyber risk.
- 4 It was noted that engagement on this topic would help to flush out HMG's appetite for such a scheme and potentially avoid a lot of further work done in vain. If HMG had appetite to engage there was no commitment from the industry to follow through should HMG seek to take the proposals in a direction the industry could not support.
- 5 Engagement with HMG on this topic could also form part of a broader conversation about the value of insurance in enhancing cyber and national resilience more generally.

POOLRe
REINSURING TERRORISM RISK

