

RESEARCH SUMMARY

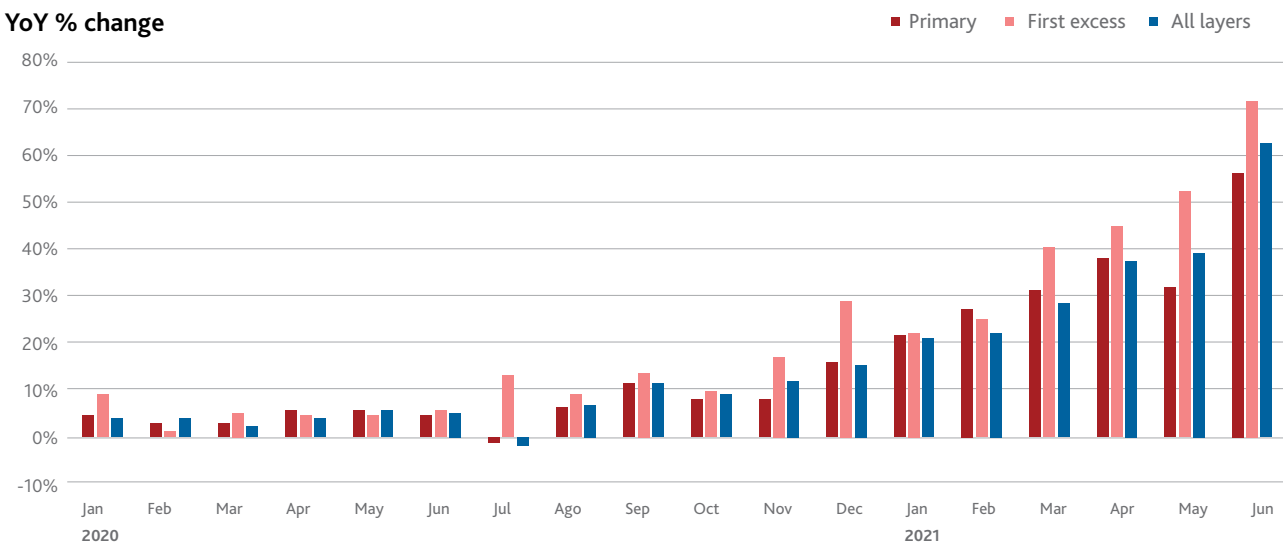
Insuring Hostile Cyber Activity:
In search of sustainable solutions

Rachel Anne Carter, Managing Director, Carter Insurance Innovations
Darren Pain, Director Cyber and Evolving Liability, The Geneva Association
Julian Enoizi, CEO, Pool Re, and Secretary, International Forum of Terrorism Risk (Re)Insurance Pools

The cyber landscape is evolving rapidly, with digitalisation expanding the range of threats and vulnerabilities. This process is amplified by shifts in working and business practices brought on by COVID-19, some of which are likely to persist beyond the pandemic. Ransomware and supply chain attacks in particular have become more prolific since the onset of the pandemic and with them wider recognition of the potential for large-scale economic disruption from malicious cyber incidents.

A dedicated market for cyber insurance has developed over time involving a progressive broadening in the class of risks covered, both first- and third-party losses. However, the recent sharp increase in loss ratios on standalone cyber insurance – i.e. dedicated affirmative cover – has prompted re/insurers to re-calibrate cyber risks. Coupled with initiatives to remove unintentional cyber exposure from conventional property and casualty policies (non-affirmative or 'silent' cyber), market re/insurance capacity has become scarcer. In the face of continuing strong demand, this has triggered a sharp rerating in the cost of cyber insurance and a tightening in terms and conditions (Figure 1).

Figure 1: Cyber insurance premium rate increases over the course of contract renewals, by layer of cover



In cyber insurance markets such as the U.S., insureds that desire more than USD 10 or USD 15 million in coverage typically layer or stack insurers. The first layer (or primary policy) will set the general terms and conditions for the entire programme. Excess policies provide any needed additional limit. The primary insurer bears 100% of the risk of loss up to its limit. Then, the first excess insurer will bear 100% of its layer, and so on.

Source: Aon¹

1 Aon 2021.

Hostile cyber activity (HCA) and insurance

Recent, serious supply chain intrusions and ransomware incidents have underscored a long-standing issue for cyber insurers: how much protection can and should insurance provide when the perpetrators of such attacks are linked to nation states? Traditional policy exclusions for war or war-like incidents fail to adequately capture situations where nation states are suspected of being behind an attack or at least providing a safe harbour for the hackers, especially if the motives for the attack are unclear. Such issues of attribution and characterisation create significant contractual uncertainty for insurers, which has only added to the recent tightening in cyber insurance market conditions.

More granular classifications of cyber incidents – including HCA terminology, which provides for a lower burden of proof for state involvement than current, widely-used definitions – will help provide greater clarity for insurers and increase comfort levels with their exposure. But market acceptance of tighter policy language over insured cyber incidents takes time and even then, will likely only go so far.

The latest cyber incidents highlight the residual challenges in creating clear-cut, definitive boundaries around what

legitimately falls within HCA and what does not. Nation-state involvement varies widely, from reported tacit sponsorship, including fostering an environment for developing sophisticated yet easy-to-use malware (e.g. the attack on Colonial Pipeline), to alleged, outright supervision and resourcing of hacking campaigns by a sovereign government (e.g. SolarWinds). In such circumstances, some of the difficulties of direct attribution for HCA resurface, particularly if state actors linked to criminal gangs use false-flag tactics to hide their traces, blame others or otherwise undermine any international consensus about the ultimate source of the attack.

Quantifying cyber risks remains challenging

Advances in modelling and the quantification of cyber risks, as well as reinsurance availability and other mechanisms to share risks, will be key to encouraging both incumbent and prospective insurers to offer increased coverage for HCA and other malicious cyber activity. Unlike for natural catastrophe perils – for example, hurricanes or man-made disasters such as terrorist attacks – cyber perils have no geographical borders; the whole world is potentially one cyber catastrophe zone. Beyond issues of attribution and characterisation, assessing the frequency and severity of HCA, especially the potential for large accumulated losses, remains a particularly serious challenge.

Table 1: Existing cyber risk scenario analysis

Scenario	Broad impact	Insurability	Uncertainty of loss estimate	Economic loss estimate (USD billion)	Insured loss estimate (USD billion)
Widespread contagious malware spread ²	Disruptive	Insured / insurable by the cyber market	High	193	27
Major cloud outage ⁽¹⁾	Disruptive	Insured / insurable by the cyber market	High	53	8
Infrastructure disruption or failure (e.g. power outage) ⁽²⁾	Destructive / disruptive	Not insured / insurable for the cyber market, exposure	Very high	1,024	71 (driven by non-affirmative exposure mainly in property)

Notes: (1) Proximate causes for the unavailability are numerous, including technical failures, distributed denial-of-service (DDoS) attacks as well as malware infections. In addition, the scenario also considers the inability of the affected customer to restore the services by themselves.³ (2) Possible triggers causing a blackout include well-known physical perils (such as severe storms or earthquakes), human errors but also malicious acts.⁴

Source: The Geneva Association and Munich Re

² Lloyd's and University of Cambridge 2019.

³ Lloyd's and Cyence 2017.

⁴ Lloyd's and University of Cambridge 2015.

Deterministic scenario analysis suggests some malicious cyber incidents, such as a temporary disruption to cloud services, might trigger economic losses broadly comparable with some historical natural catastrophes (Table 1). But more extreme and long-lasting cyberattacks, including a widespread IT or operational infrastructure outage or failure, could generate significantly larger expected losses. Moreover, the uncertainty surrounding such estimates is very large, meaning that total potential losses could be significantly higher than these 'guesstimates', easily exhausting re/insurers' risk-absorbing capacity. This is especially true of HCA incidents where ambiguity over hackers' motives, tactics and threat vectors, as well as the possibility for relatively minor, isolated attacks to escalate towards full-out cyber warfare, only add to the complications of quantifying cyber risks.

The role of a government backstop

Advances in gathering cyber threat intelligence, including collaboration across firms and governments, will boost risk awareness and preparedness, important elements in building cyber resilience. Such information will enable insurers to detect vulnerabilities and foster improvements in modelling cyber risks. Likewise, progress by law enforcement agencies in tracing and pursuing the perpetrators of an attack and recovering extorted funds may go some way to deterring cyber criminals and increasing insurers' comfort levels in offering risk-absorbing capacity.

Ultimately, however, the systemic characteristic of some cyber risks, in particular the potential for multiple losses from a single event or a campaign of attacks linked to HCA, mean that the scale of accumulated losses may exceed levels that can safely and sensibly be absorbed by the private re/insurance sector. There is often collateral damage surrounding a large-scale, malicious cyberattack; unintended targets also suffer loss. To some extent too, the latest spate of attacks can be seen as near-misses; if circumstances had transpired differently the losses could have been much worse.

Echoing current debates over pandemic-related risks, consideration should thus be given to government-backed solutions to finance these tail cyber risks in order to boost economy-wide resilience. A well-designed public-private partnership (PPP) could increase protection capacity and still encourage cyber market innovations to extend cover for HCA risks. This should not simply be a fiscal solution but also seek, through collaboration with insurers, to promote the adoption of cybersecurity best practices – including taking out appropriate insurance – to reduce societal vulnerability to such risks.





Designing a PPP

Designing such government-backed solutions is complex. Important considerations for any PPP include whether the scheme is mandatory or voluntary, coverage is parametric or indemnity-based or if the scheme is founded upon mutuality or solidarity principles. From a fiscal and feasibility viewpoint, it will also be necessary to ensure that adequate measures are adopted to fund the scheme and to ensure sufficient capital, either on a pre- or post-event basis. There will be trade-offs in adopting particular scheme features and difficulties in calibrating how much of the peak losses should be shared among policyholders, private re/insurers and governments (Table 2).

Such design challenges are amplified at the international level. Ideally, given the interconnected and global nature of cyber risks, cooperative international solutions to cover HCA risks would be an option. However, legal limitations, cultural differences, access to capital and doubts about the willingness of individual governments to share risks across different jurisdictions mean that global solutions remain practically infeasible, at least in the short term. As a result, priority should be given to developing domestic PPP solutions for large-scale cyber risks.

The insurance industry has come a long way in its understanding of cyber terrorism, HCA and cyber war and assessing how to insure such risks. To expand the limits of insurability, insurers need to be proactive in assessing feasible options for sharing cyber risks, including with governments via PPPs. Such collaborative efforts between insurers and governments will enable cyber protection gaps to be narrowed and ensure the full societal benefits of cyberspace can be realised.

Table 2: Summary of the pros/cons of possible features of a PPP scheme

Scheme feature	Possible pros and cons
 <p>Multi-peril (versus single peril)</p>	<p>Pro: Diversification opportunities</p> <p>Con: Higher administration costs</p>
 <p>Mandatory (versus voluntary)</p>	<p>Pro: Enlarges the premium pool and avoids adverse selection</p> <p>Con: Complex to monitor and enforce compliance</p>
 <p>Pre-funded (versus post-funded)</p>	<p>Pro: Incentivises risk prevention and mitigation and funds on-hand for disbursement</p> <p>Con: Political support to fund a contingency can often be challenging</p>
 <p>Parametric (versus indemnity-based)</p>	<p>Pro: Provides post-event liquidity faster and more efficiently</p> <p>Con: Payout may differ from the actual losses incurred</p>
 <p>Solidarity (versus mutuality principles)</p>	<p>Pro: Boosts cyber insurance to those who might otherwise be unable to afford it</p> <p>Con: Often requires comprehensiveness and compulsion</p>
 <p>Permanent (versus temporary)</p>	<p>Pro: Develops a long-term strategy for securing funding as well as accumulating capital</p> <p>Con: Potentially crowds out private market participants and stifles potential future innovation</p>

Source: The Geneva Association

References

Aon. 2021. *Cyber Insurance Snapshot. A Focused View of 2021 Risk and Insurance Challenges.*

Lloyd’s and Cyence. 2017. *Counting the Cost. Cyber Exposure Decoded.*

Lloyd’s and University of Cambridge. 2015. *Business Blackout. Insurance Implications of a Cyber Attack on the US Power Grid.*

Lloyd’s and University of Cambridge. 2019. *Bashe Attack. Global Infection by Contagious Malware.*